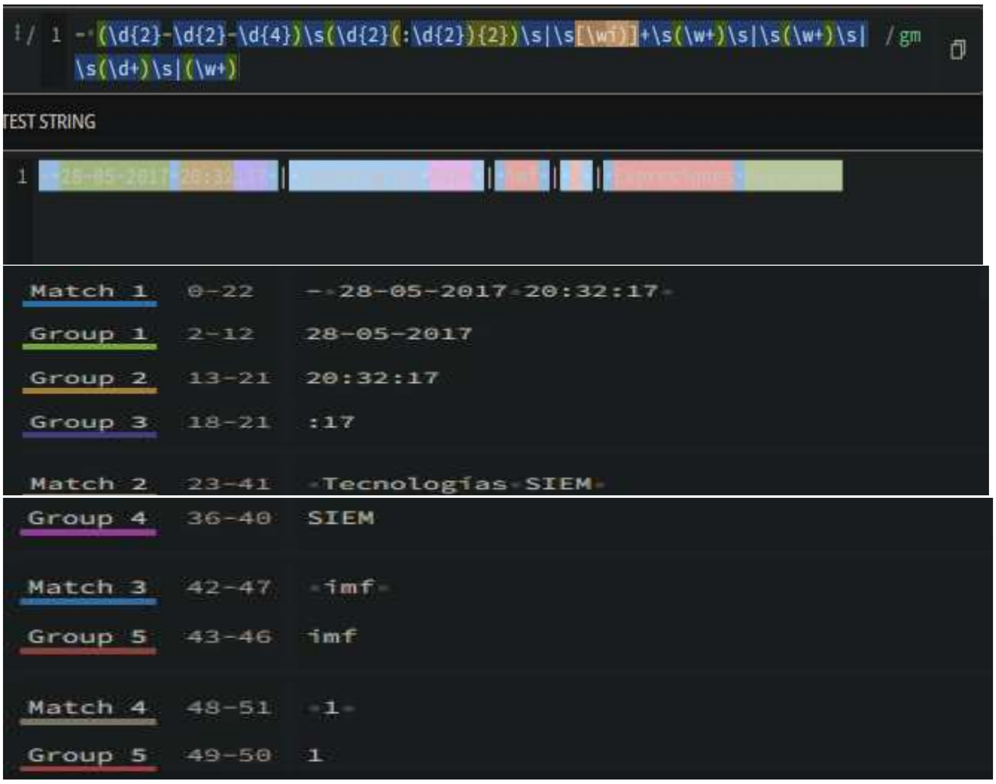
EJERCICIO REGEX

En los ejercicios siguientes se ha utilizado la herramienta online https://regex101.com/ para su resolución.

--- Ejercicio 1.- Desarrolla la expresión regular que parsee el siguiente log:

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

✓ RESOLUCIÓN:



```
/ 1 - (\d{2}-\d{2}-\d{4})\s(\d{2}(:\d{2}){2})\s|\s[\wí)]+\s(\w+)\s|\s(\w+)\s|   /gm
    \s(\d+)\s|(\w+)
```

TEST STRING

```
Match 1    0-22     - 28-05-2017 20:32:17
Group 1    2-12     28-05-2017
Group 2    13-21    20:32:17
Group 3    18-21    :17

Match 2    23-41    Tecnologías SIEM
Group 4    36-40    SIEM

Match 3    42-47    imf
Group 5    43-46    imf

Match 4    48-51    1
Group 5    49-50    1
```

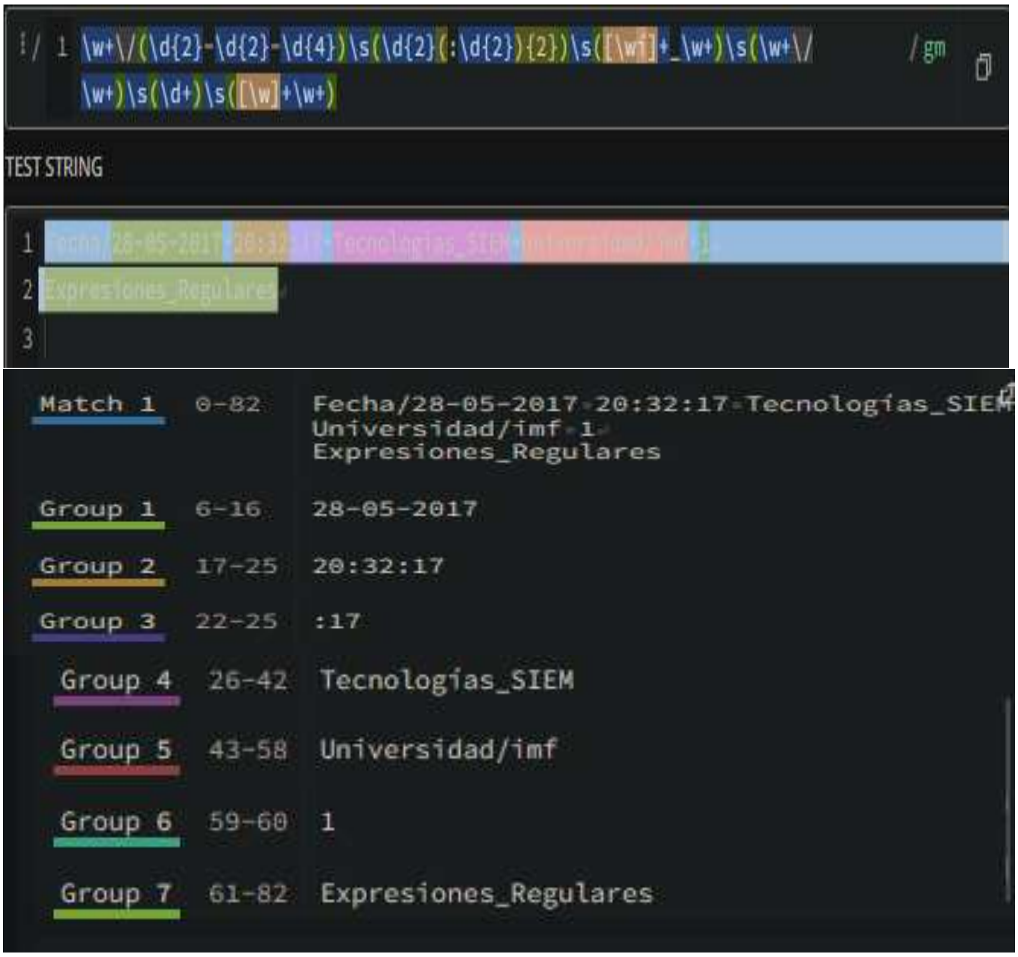
EXPRESIÓN REGULAR:

- (\d{2}-\d{2}-\d{4})\s(\d{2}(:\d{2}){2})\s|\s[\wí)]+\s(\w+)\s|\s(\w+)\s|\s(\d+)\s|(\w+)

--- Ejercicio 2.- Desarrolla la expresión regular que parsee el siguiente log:

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

✓ *RESOLUCIÓN:*



```
\w+\/(\d{2}-\d{2}-\d{4})\s(\d{2}(:\d{2}){2})\s([\wí]+_\w+)\s(\w+\/
\w+)\s(\d+)\s([\w]+\w+)                                          /gm

TEST STRING

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

Match 1    0-82    Fecha/28-05-2017 20:32:17 Tecnologías_SIEM
                   Universidad/imf 1
                   Expresiones_Regulares

Group 1    6-16    28-05-2017

Group 2    17-25   20:32:17

Group 3    22-25   :17

Group 4    26-42   Tecnologías_SIEM

Group 5    43-58   Universidad/imf

Group 6    59-60   1

Group 7    61-82   Expresiones_Regulares
```

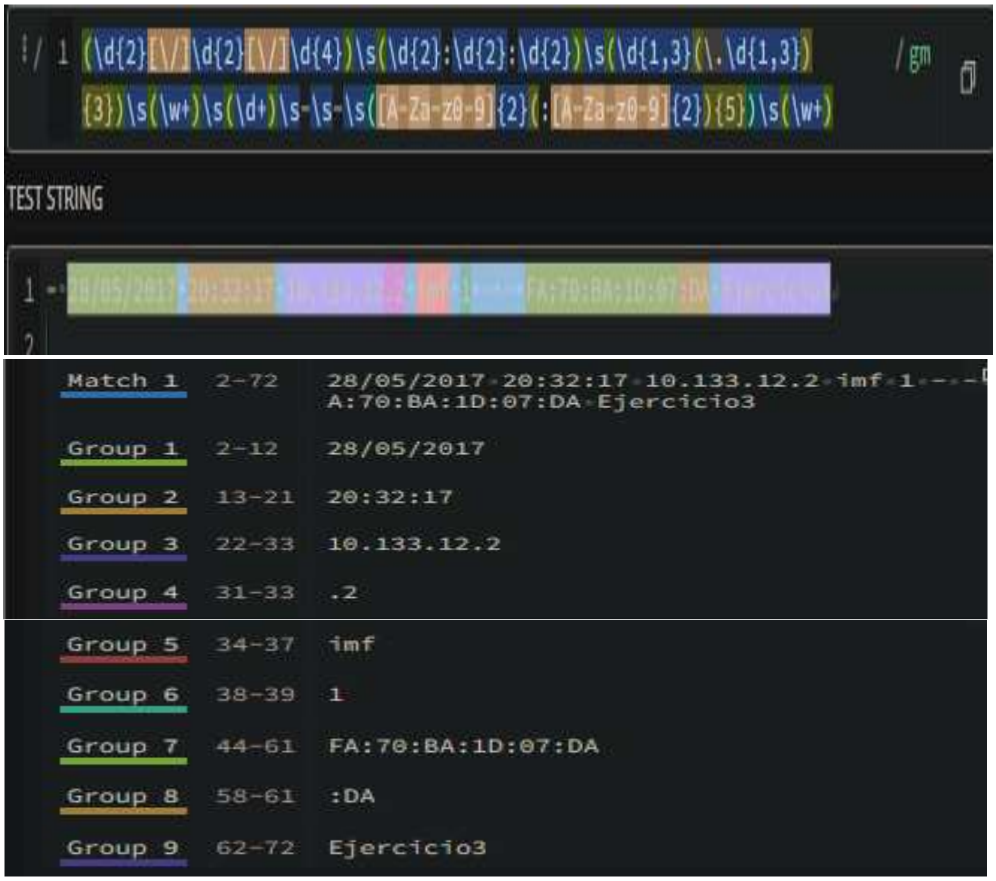
EXPRESIÓN REGULAR:

/\w+\/(\d{2}-\d{2}-\d{4})\s(\d{2}(:\d{2}){2})\s([\wí]+_\w+)\s(\w+\/\w+)\s(\d+)\s([\w]+\w+) /gm

--- Ejercicio 3.- Desarrolla 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*

✓ RESOLUCION:



```
/ (\d{2}[\/]\d{2}[\/]\d{4})\s(\d{2}:\d{2}:\d{2})\s(\d{1,3}(\.\d{1,3})
  {3})\s(\w+)\s(\d+)\s-\s-\s([A-Za-z0-9]{2}(:[A-Za-z0-9]{2}){5})\s(\w+)      / gm
```

TEST STRING

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

```
Match 1    2-72    28/05/2017 20:32:17 10.133.12.2 imf 1 - - F
                   A:70:BA:1D:07:DA Ejercicio3

Group 1    2-12    28/05/2017

Group 2    13-21   20:32:17

Group 3    22-33   10.133.12.2

Group 4    31-33   .2

Group 5    34-37   imf

Group 6    38-39   1

Group 7    44-61   FA:70:BA:1D:07:DA

Group 8    58-61   :DA

Group 9    62-72   Ejercicio3
```

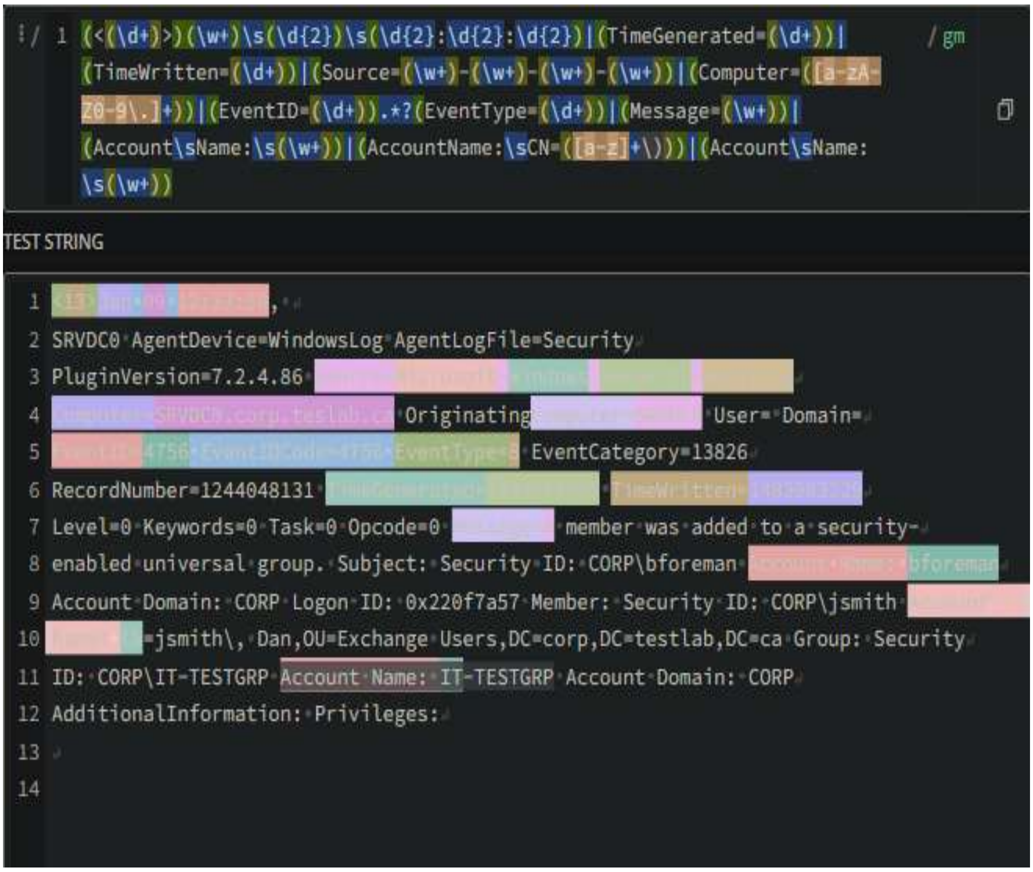
EXPRESIÓN REGULAR:

/(\d{2}[\/]\d{2}[\/]\d{4})\s(\d{2}:\d{2}:\d{2})\s(\d{1,3}(\.\d{1,3}){3})\s(\w+)\s(\d+)\s-\s-\s([A-Za-z0-9]{2}(:[A-Za-z0-9]{2}){5})\s(\w+)/gm

--- 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 AdditionalInformation: Privileges:*

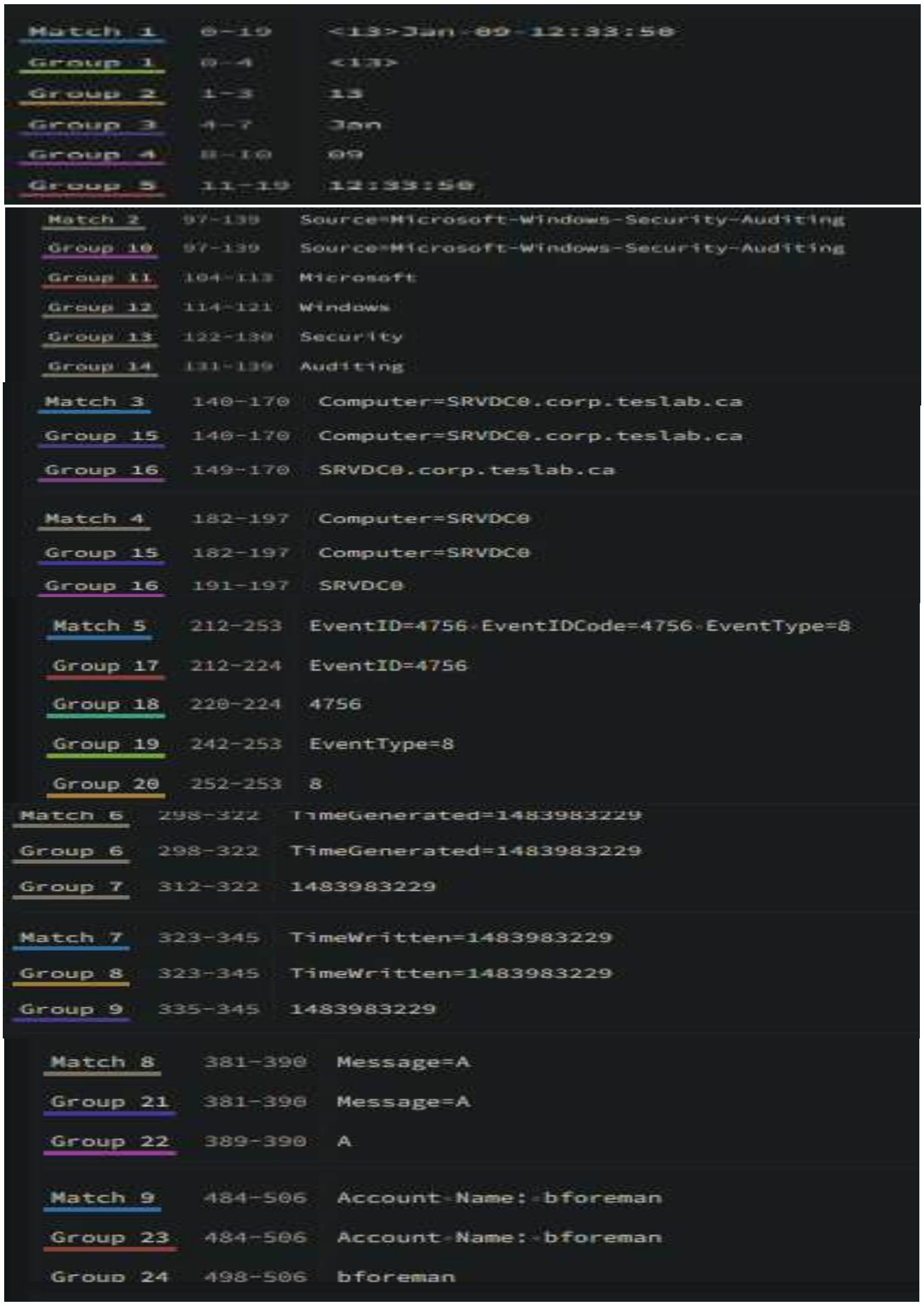
✓ RESOLUCIÓN:



```
/ ((<(\d+)>)(\w+)\s(\d{2})\s(\d{2}:\d{2}:\d{2})|(TimeGenerated=(\d+))|(TimeWritten=(\d+))|(Source=(\w+)-(\w+)-(\w+)-(\w+))|(Computer=([a-zA-Z0-9\.]+))|(EventID=(\d+)).*?(EventType=(\d+))|(Message=(\w+))|(Account\sName:\s(\w+))|(AccountName:\sCN=([a-z]+\)))|(Account\sName:\s(\w+)) /gm
```

TEST STRING

```
<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
AdditionalInformation: Privileges:
```



```
Match 1     0-19      <13>Jan 09 12:33:58
Group 1     0-4       <13>
Group 2     1-3       13
Group 3     4-7       Jan
Group 4     8-10      09
Group 5     11-19     12:33:58
Match 2     97-139    Source=Microsoft-Windows-Security-Auditing
Group 10    97-139    Source=Microsoft-Windows-Security-Auditing
Group 11    104-113   Microsoft
Group 12    114-121   Windows
Group 13    122-130   Security
Group 14    131-139   Auditing
Match 3     140-170   Computer=SRVDC0.corp.teslab.ca
Group 15    140-170   Computer=SRVDC0.corp.teslab.ca
Group 16    149-170   SRVDC0.corp.teslab.ca

Match 4     182-197   Computer=SRVDC0
Group 15    182-197   Computer=SRVDC0
Group 16    191-197   SRVDC0
Match 5     212-253   EventID=4756 EventIDCode=4756 EventType=8
Group 17    212-224   EventID=4756
Group 18    220-224   4756
Group 19    242-253   EventType=8
Group 20    252-253   8
Match 6     298-322   TimeGenerated=1483983229
Group 6     298-322   TimeGenerated=1483983229
Group 7     312-322   1483983229

Match 7     323-345   TimeWritten=1483983229
Group 8     323-345   TimeWritten=1483983229
Group 9     335-345   1483983229
Match 8     381-390   Message=A
Group 21    381-390   Message=A
Group 22    389-390   A

Match 9     484-506   Account Name: bforeman
Group 23    484-506   Account Name: bforeman
Group 24    498-506   bforeman
```

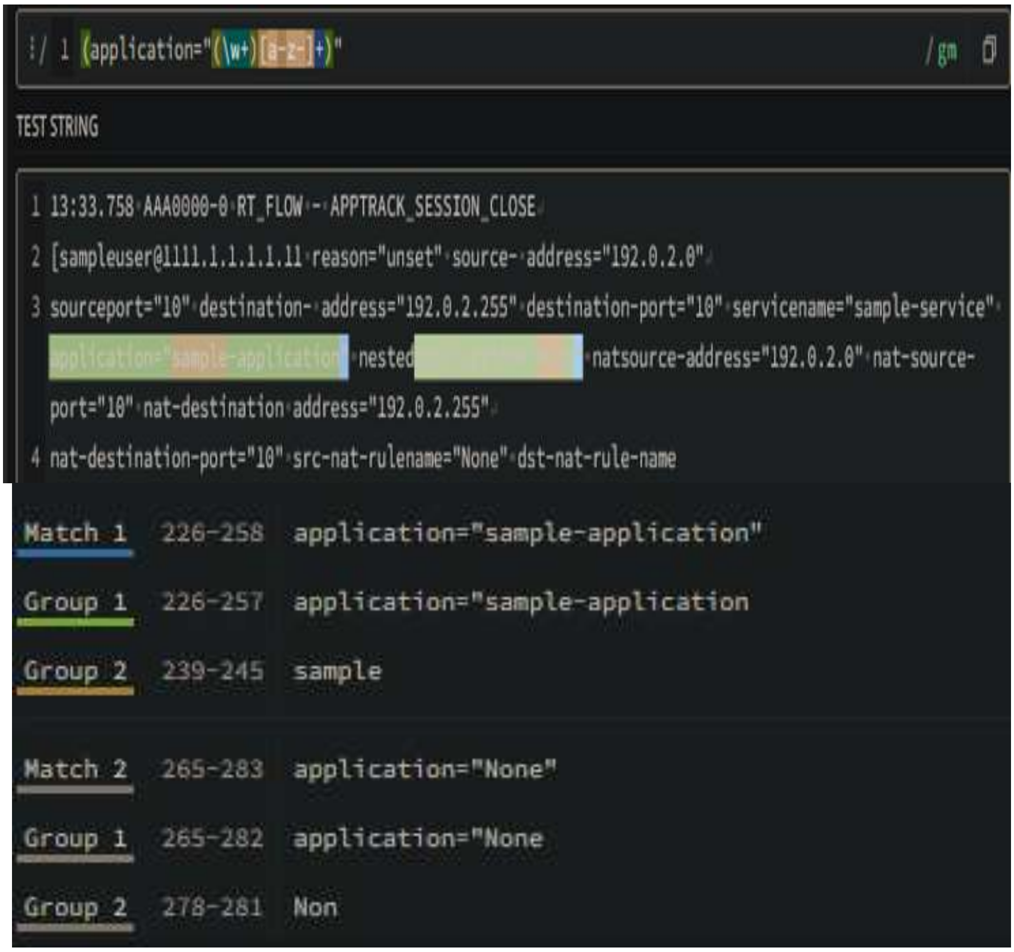
- EXPRESIÓN REGULAR:

```
/(<(\d+)>)(\w+)\s(\d{2})\s(\d{2}:\d{2}:\d{2})|(TimeGenerated=(\d+))|(TimeWritten=(\d+))|(Source=(\w+)-(\w+)-(\w+)-(\w+))|(Computer=([a-zA-Z0-9\.]+))|(EventID=(\d+)).*?(EventType=(\d+))|(Message=(\w+))|(Account\sName:\s(\w+))|(AccountName:\sCN=([a-z]+\)))|(Account\sName:\s(\w+))/gm
```

--- Ejercicio 5.- Desarrollar la expresión regular que parsee del siguiente log de QRadar 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"
  sourceport="10" destination- address="192.0.2.255" destination-port="10"
  service-
  name="sample-service" application="sample-application"
  nestedapplication="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-rulename="None" dst-nat-rule-name

✓ RESOLUCION:



```
/ (application="(\w+)[a-z-]+)"                                    /gm
```

TEST STRING

```
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"
sourceport="10" destination- address="192.0.2.255" destination-port="10" servicename="sample-service"
application="sample-application nested[illegible] natsource-address="192.0.2.0" nat-source-
port="10" nat-destination address="192.0.2.255"
nat-destination-port="10" src-nat-rulename="None" dst-nat-rule-name
```

```
Match 1   226-258   application="sample-application"
Group 1   226-257   application="sample-application
Group 2   239-245   sample

Match 2   265-283   application="None"
Group 1   265-282   application="None
Group 2   278-281   Non
```

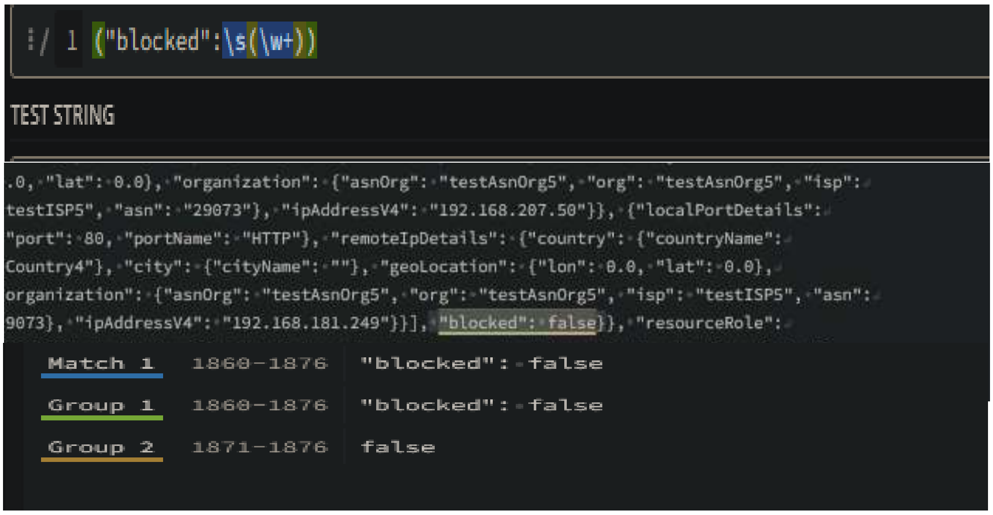
EXPRESIÓN REGULAR:

/(application="(\w+)[a-z-]+)"/gm

--- Ejercicio 6.- Desarrollar la expresión regular que parsee del siguiente log de QRadar si el stream ha sido bloqueado o no (campo blocked)

```
LogStreamName: GuardDutyLogStream,Timestamp:
1537272809958,Message: {"version":
"0", "id": "095aab52-d1cd-2a72-a11a-afda5b22c1f6", "detailtype":
"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/24b2e6fc47
df1e5186fc306f75130143", "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:
34282329235502547611359803964175423399678929446014877696}
```

✓ *RESOLUCIÓN:*



```
("blocked":\s(\w+))
```

TEST STRING

```
.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":
9073}, "ipAddressV4": "192.168.181.249"}}], "blocked": false}}, "resourceRole":
```

```
Match 1    1860-1876   "blocked": false
Group 1    1860-1876   "blocked": false
Group 2    1871-1876   false
```

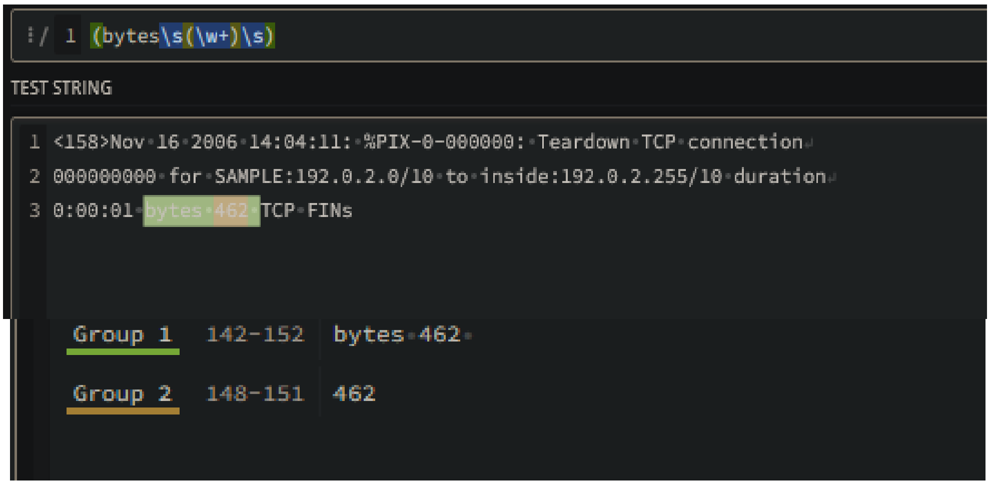
EXPRESIÓN REGULAR:

/("blocked":\s(\w+))/gm

--- Ejercicio 7.- Desarrollar la expresión regular que parsee del siguiente log de QRadar el número de bytes de la conexión (campo bytes)

- *<158>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*

✓ *RESOLUCIÓN:*



```
(bytes\s(\w+)\s)
```

TEST STRING

```
<158>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
```

```
Group 1    142-152   bytes 462
Group 2    148-151   462
```

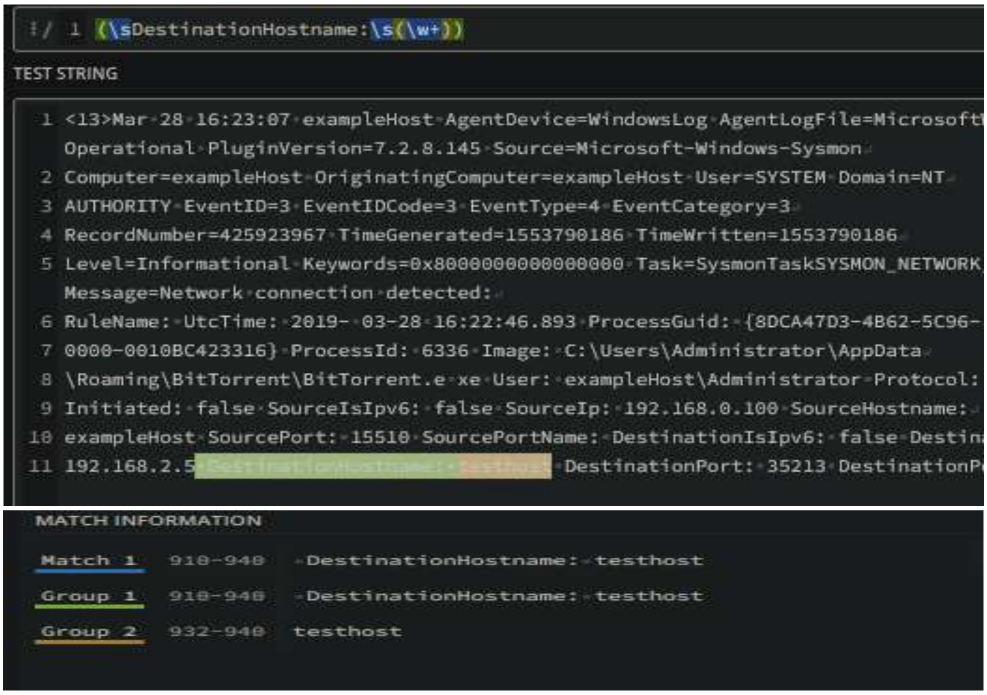
EXPRESIÓN REGULAR:

/(bytes\s(\w+)\s)/gm

--- <u>Ejercicio 8</u>.- Desarrollar la expresión regular que parsee del siguiente log de QRadar 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.e xe 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:*

✓ RESOLUCIÓN:



```
(\sDestinationHostname:\s(\w+))
```

TEST STRING

```
<13>Mar 28 16:23:07 exampleHost AgentDevice=WindowsLog AgentLogFile=Microsoft
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=SysmonTaskSYSMON_NETWORK
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.e xe User: exampleHost\Administrator Protocol:
Initiated: false SourceIsIpv6: false SourceIp: 192.168.0.100 SourceHostname:
exampleHost SourcePort: 15510 SourcePortName: DestinationIsIpv6: false Destin
192.168.2.5 DestinationHostname: testhost DestinationPort: 35213 DestinationP
```

MATCH INFORMATION

```
Match 1   918-948   DestinationHostname: testhost
Group 1   918-948   DestinationHostname: testhost
Group 2   932-948   testhost
```

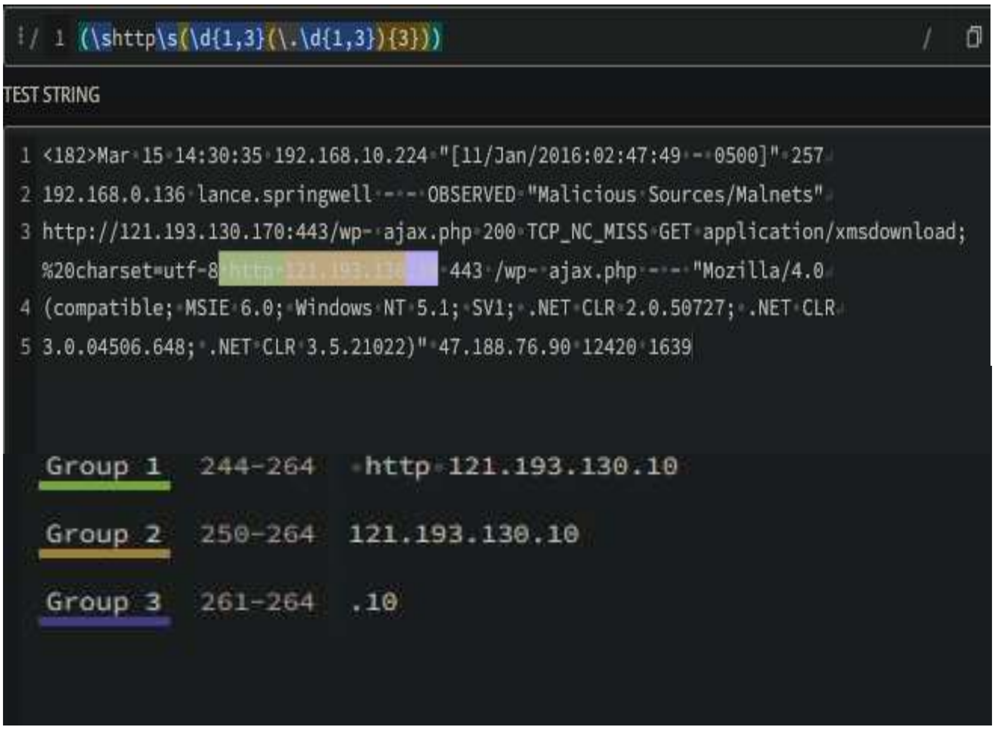
EXPRESIÓN REGULAR:

/(\sDestinationHostname:\s(\w+))/gm

--- <u>Ejercicio 9</u>.- Desarrollar la expresión regular que parsee del siguiente log de QRadar 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

✓ *RESOLUCIÓN:*



```
/ (\shttp\s(\d{1,3}(\.\d{1,3}){3})) /
```

TEST STRING

```
<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/xmsdownload;
%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
```

```
Group 1   244-264    http 121.193.130.10
Group 2   250-264   121.193.130.10
Group 3   261-264   .10
```

EXPRESIÓN REGULAR:

/(\shttp\s(\d{1,3}(\.\d{1,3}){3}))/