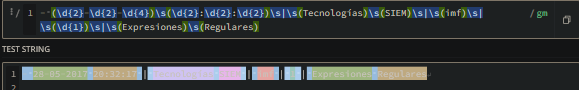
Ejercicio 1.- Desarrolla la expresión regular que parsee el siguiente log:

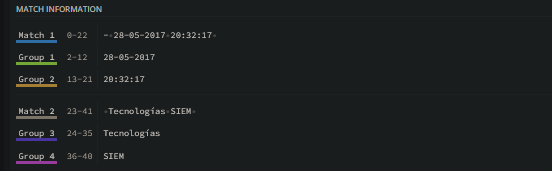
LOG:

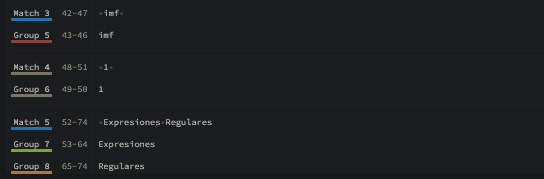
* *- 28-05-2017 20:32:17 | Tecnologías SIEM | imf | 1 | Expresiones Regulares*

**RESOLUCIÓN:**

**/- (\d{2}-\d{2}-\d{4})\s(\d{2}:\d{2}:\d{2})\s|\s(Tecnologías)\s(SIEM)\s|\s(imf)\s|\s(\d{1})\s|\s(Expresiones)\s(Regulares)/gm**

****

****

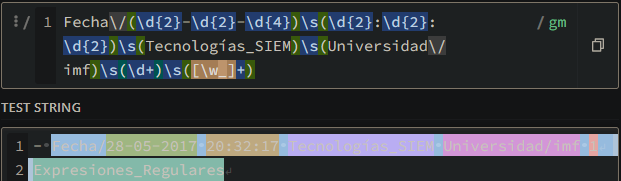
****

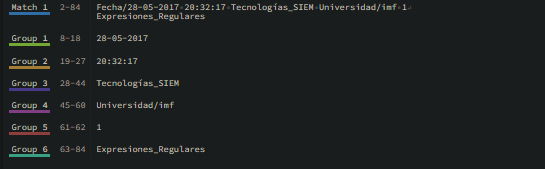
Ejercicio 2.- Desarrolla la expresión regular que parsee el siguiente log:

* *- Fecha/28-05-2017 20:32:17 Tecnologías\_SIEM Universidad/imf 1  
  Expresiones\_Regulares*

*RESOLUCIÓN:*

*/Fecha\/(\d{2}-\d{2}-\d{4})\s(\d{2}:\d{2}:\d{2})\s(Tecnologías\_SIEM)\s(Universidad\/imf)\s(\d+)\s([\w\_]+)/gm*

**

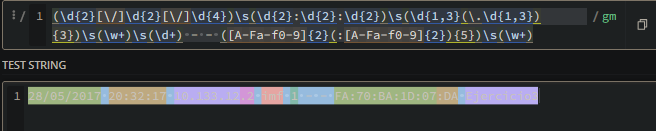
**

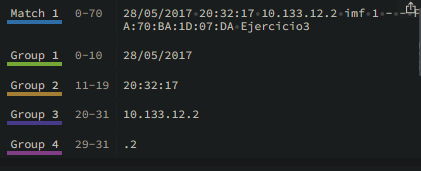
Ejercicio 3.- Desarrolla la expresión regular que parsee el siguiente log:

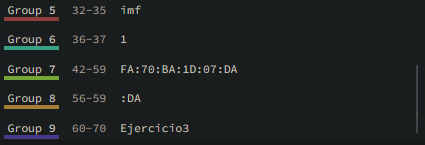
* *- 28/05/2017 20:32:17 10.133.12.2 imf 1 - - FA:70:BA:1D:07:DA Ejercicio3*

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+) - - ([A-Fa-f0-9]{2}(:[A-Fa-f0-9]{2}){5})\s(\w+)







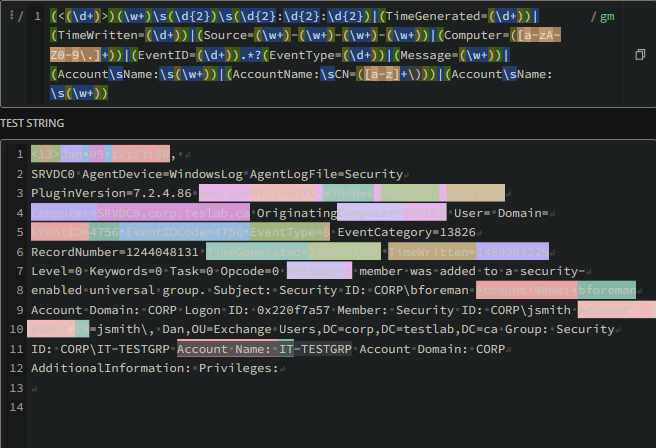
Ejercicio 4.- Extraer del siguiente log los siguientes campos:

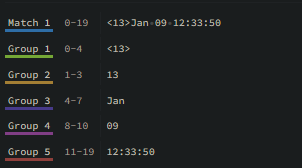
timestamp,src.hostname, event.id, event.type, message, attacker.username,target.username, target.groupname

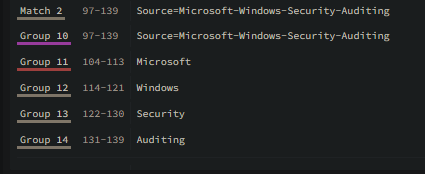
* *<13>Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security  
  PluginVersion=7.2.4.86 Source=Microsoft-Windows-Security-Auditing  
  Computer=SRVDC0.corp.teslab.ca OriginatingComputer=SRVDC0 User= Domain=  
  EventID=4756 EventIDCode=4756 EventType=8 EventCategory=13826  
  RecordNumber=1244048131 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:

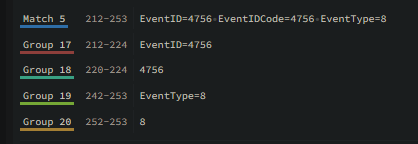
/(<(\d+)>)(\w+)\s(\d{2})\s(\d{2}:\d{2}:\d{2})|(TimeGenerated=(\d+))|(TimeWritten=(\d+))|(Source=(\w+)-(\w+)-(\w+)-(\w+))|(Computer=([a-zA-Z0-9\.]+))|(EventID=(\d+)).\*?(EventType=(\d+))|(Message=(\w+))|(Account\sName:\s(\w+))|(AccountName:\sCN=([a-z]+\)))|(Account\sName:\s(\w+))/gm

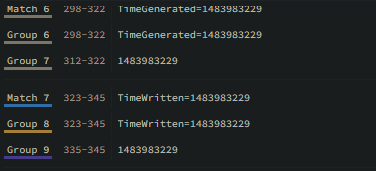


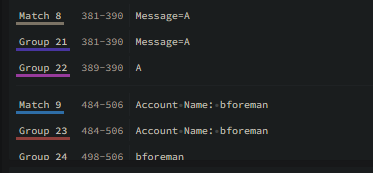










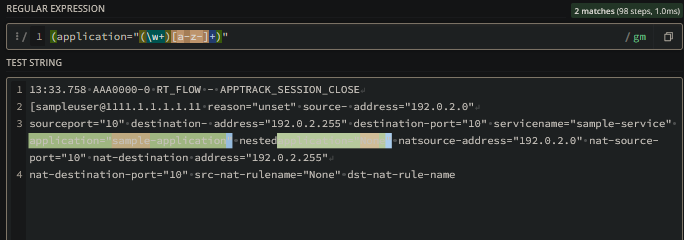


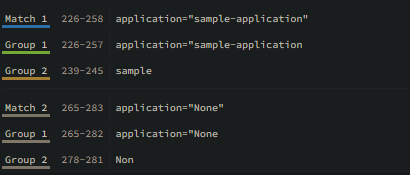
Ejercicio 5.- Desarrollar la expresión regular que parsee del siguiente log de QRadar la cadena:

* *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





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}*

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*

Ejercicio 8.- Desarrollar la expresión regular que parsee del siguiente log de QRadarel 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:*

Ejercicio 9.- 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*