REST SDK how to example: how to get pcap for any query and how to get meta values for any particular session on a concentrator or broker:

1) use REST /sdk/query to get sessionids for any query;

2) then use REST /sdk/packets to get pcap for matching sessions;

3) then use REST /sdk/session to get meta id ranges for a single session (or consecutive sessions);

4) then use REST /sdk/query to get meta values for a single session (or consecutive sessions).

Example:

Here is an actual /sdk/query to select sessionid where ip.src=10.194.238.251 and alias.host=time.vocalocity.com and time from 12/6/2012 8am to 12/6/2012 9am:
Parameters: query="select sessionid where time='2012-Dec-06 08:00:00'-'2012-Dec-06 09:00:00'&&ip.src=10.194.238.251&&alias.host=time.vocalocity.com" size=100

Note: this query will return all matching sessionids for the query.

Here is the matching URL encoded (http://www.w3schools.com/tags/ref_urlencode.asp) REST /sdk/query for 10.25.53.20 concentrator:
http://10.25.53.20:50105/sdk?msg=query&query=select+sessionid+where+time%3D%272012-Dec-06+08%3A00%3A00%27-%272012-Dec-06+09%3A00%3A00%27%26%26ip.src%3D10.194.238.251%26%26alias.host%3Dtime.vocalocity.com&force-content-type=text/xml&size=100

1) Run above REST /sdk/query on 10.25.53.20 concentrator (using default login credentials: admin/netwitness) with curl command below:

```
[root@Concentrator10.25.53.20 ~]# curl --user 'admin:netwitness' 'http://10.25.53.20:50105/sdk?msg=query&query=select+sessionid+where+time%3D%272012-Dec-06+08%3A00%3A00%27-%272012-Dec-06+09%3A00%3A00%27%26%26ip.src%3D10.194.238.251%26%26alias.host%3Dtime.vocalocity.com&force-content-type=text/plain&size=100'
[id1=833454200  id2=833454199
id1=327817978  id2=327817978  count=0  format=8  value=7961890  type=sessionid  flags=0  group=7961890
id1=328152871  id2=328152871  count=0  format=8  value=7971028  type=sessionid  flags=0  group=7971028
id1=328480455  id2=328480455  count=0  format=8  value=7979891  type=sessionid  flags=0  group=7979891
id1=328819956  id2=328819956  count=0  format=8  value=7988888  type=sessionid  flags=0  group=7988888
id1=329177836  id2=329177836  count=0  format=8  value=7998461  type=sessionid  flags=0  group=7998461
id1=330021356  id2=330021356  count=0  format=8  value=8023307  type=sessionid  flags=0  group=8023307
id1=330363917  id2=330363917  count=0  format=8  value=8032644  type=sessionid  flags=0  group=8032644
id1=330701550  id2=330701550  count=0  format=8  value=8041720  type=sessionid  flags=0  group=8041720
id1=331039517  id2=331039517  count=0  format=8  value=8050787  type=sessionid  flags=0  group=8050787
id1=331380099  id2=331380099  count=0  format=8  value=8060021  type=sessionid  flags=0  group=8060021
id1=331739773  id2=331739773  count=0  format=8  value=8069414  type=sessionid  flags=0  group=8069414
id1=332062050  id2=332062050  count=0  format=8  value=8078373  type=sessionid  flags=0  group=8078373
[root@Concentrator10.25.53.20 ~]#
```

Note that there are 12 sessionids in the output ,which means there are 12 sessions matching above query.

Note: if your query contains many sessions, you should adjust size=100 to capture all sessionids (size range: 1-1677721).

2) Run below REST /sdk/packets curl command on the same concentrator 10.25.53.20 with above 12 sessionids and pipe output to a pcap file (if consecutive sessionids, can use – in between):

```
[root@Concentrator10.25.53.20 ~]# curl --user 'admin:netwitness'
'http://10.25.53.20:50105/sdk/packets?&sessions=7961890,7971028,7979891,7988888,7998461,8023307,8032644,8041720,8050787,8060021,8069414,8078373' >
test.pcap
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2592    0  2592    0     0   2424      0 --:--:--  0:00:01 --:--:-- 37565
[root@Concentrator10.25.53.20 ~]# ll test.pcap
```

```
-rw-r--r-- 1 root root 2592 Dec  6 11:12 test.pcap
[root@Concentrator10.25.53.20 ~]#

One can also run this alternative curl command below to get the same results:
[root@Concentrator10.25.53.20 ~]# curl --user 'admin:netwitness' -o test1.pcap --data
"render=pcap&sessions=7961890,7971028,7979891,7988888,7998461,8023307,8032644,8041720,8050787,8060021,8069414,8078373"
'http://10.25.53.20:50105/sdk/packets'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2592    0  2592    0     0   2796      0 --:--:-- --:--:-- --:--:-- 2411k
[root@Concentrator10.25.53.20 ~]# ll test*
-rw-r--r-- 1 root root 2592 Dec  7 10:00 test1.pcap
-rw-r--r-- 1 root root 2592 Dec  6 11:12 test.pcap

One can also run this alternative curl command below to get the same results:
[root@Concentrator10.25.53.20 ~]# curl --user 'admin:netwitness' -o test2.pcap
'http://10.25.53.20:50105/sdk/packets?&sessions=7961890,7971028,7979891,7988888,7998461,8023307,8032644,8041720,8050787,8060021,8069414,8078373&reder=pcap
'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2592    0  2592    0     0   187k      0 --:--:-- --:--:-- --:--:-- 1205k
[root@Concentrator10.25.53.20 ~]# ll test*
-rw-r--r-- 1 root root 2592 Dec  7 10:00 test1.pcap
-rw-r--r-- 1 root root 2592 Dec 10 09:57 test2.pcap
-rw-r--r-- 1 root root 2592 Dec  6 11:12 test.pcap
[root@Concentrator10.25.53.20 ~]#
```

3) To get all meta values for a specific session, first, run below REST /sdk/session curl command on the same concentrator 10.25.53.20 for the desired sessionid obtained from 1) above (7961890), which will return meta id ranges for the session in field1 and field2 below (meta id values for a session are always consecutive!):

```
[root@Concentrator10.25.53.20 ~]# curl --user "admin:netwitness" 'http://10.25.53.20:50105/sdk?msg=session&id2=7961890&id1=7961890&&force-content-
type=text/plain'
id1: 7961890
id2: 7961890
field1: 327817978
field2: 327818016
```

4) Now, run below REST /sdk/query curl command against the same concentrator 10.25.53.20 with the meta id ranges returned from above command to get all meta values for this specific session (7961890) and pipe to an xml file for later review:

```
[root@CSO-Conc-S3-SM64-20 ~]# curl --user "admin:netwitness" 'http://10.25.53.20:50105/sdk?msg=query&force-content-
type=text/xml&id1=327817978&id2=327818016&query=select%20*&size=500' > session7961890metavalues.xml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5265  100  5265    0     0   672k      0 --:--:-- --:--:-- --:--:--     0
[root@Concentrator10.25.53.20 ~]# ll session7961890metavalues.xml
-rw-r--r-- 1 root root 5265 Dec 13 14:58 session7961890metavalues.xml
[root@Concentrator10.25.53.20 ~]# cat session7961890metavalues.xml
<?xml version="1.0" encoding="utf-8"?>
<response flags="1074200577">
        <results id1="327818017" id2="327818016">
                <field count="0" flags="0" format="8" group="7961890" id1="327817978" id2="327817978" size="8" type="sessionid">7961890</field>
                <field count="0" flags="0" format="32" group="7961890" id1="327817979" id2="327817979" size="8" type="time">1354780922</field>
                <field count="0" flags="0" format="6" group="7961890" id1="327817980" id2="327817980" size="4" type="size">182</field>
                <field count="0" flags="0" format="6" group="7961890" id1="327817981" id2="327817981" size="4" type="payload">90</field>
                <field count="0" flags="0" format="2" group="7961890" id1="327817982" id2="327817982" size="1" type="medium">1</field>
                <field count="0" flags="0" format="130" group="7961890" id1="327817983" id2="327817983" size="8" type="eth.src">00:04:F2:25:D4:3C</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327817984" id2="327817984" size="7" type="eth.src.vendor">Polycom</field>
                <field count="0" flags="0" format="130" group="7961890" id1="327817985" id2="327817985" size="8" type="eth.dst">00:90:FB:33:AB:C8</field>
```

```
                <field count="0" flags="0" format="65" group="7961890" id1="327817986" id2="327817986" size="14" type="eth.dst.vendor">PORTWELL,
INC.</field>
                <field count="0" flags="0" format="4" group="7961890" id1="327817987" id2="327817987" size="2" type="eth.type">2048</field>
                <field count="0" flags="0" format="128" group="7961890" id1="327817988" id2="327817988" size="4" type="ip.src">10.194.238.251</field>
                <field count="0" flags="0" format="128" group="7961890" id1="327817989" id2="327817989" size="4" type="ip.dst">4.2.2.2</field>
                <field count="0" flags="0" format="2" group="7961890" id1="327817990" id2="327817990" size="1" type="ip.proto">17</field>
                <field count="0" flags="0" format="4" group="7961890" id1="327817991" id2="327817991" size="2" type="udp.srcport">3080</field>
                <field count="0" flags="0" format="4" group="7961890" id1="327817992" id2="327817992" size="2" type="udp.dstport">53</field>
                <field count="0" flags="0" format="6" group="7961890" id1="327817993" id2="327817993" size="4" type="service">53</field>
                <field count="0" flags="0" format="2" group="7961890" id1="327817994" id2="327817994" size="1" type="streams">2</field>
                <field count="0" flags="0" format="6" group="7961890" id1="327817995" id2="327817995" size="4" type="packets">2</field>
                <field count="0" flags="0" format="4" group="7961890" id1="327817996" id2="327817996" size="2" type="lifetime">1</field>
                <field count="0" flags="0" format="128" group="7961890" id1="327817997" id2="327817997" size="4" type="alias.ip">205.139.46.10</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327817998" id2="327817998" size="19"
type="alias.host">time.vocalocity.com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327817999" id2="327817999" size="3" type="tld">com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818000" id2="327818000" size="19"
type="alias.host">time.vocalocity.com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818001" id2="327818001" size="3" type="tld">com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818002" id2="327818002" size="19"
type="alias.host">time.vocalocity.com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818003" id2="327818003" size="3" type="tld">com</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818004" id2="327818004" size="7" type="alert.id">nw05275</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818005" id2="327818005" size="21" type="risk.suspicious">dns extremely low
ttl</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818006" id2="327818006" size="10" type="threat.category">suspicious</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818007" id2="327818007" size="10" type="threat.source">netwitness</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818008" id2="327818008" size="8" type="dns.responsetype">a record</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818009" id2="327818009" size="13" type="country.dst">United States</field>
                <field count="0" flags="0" format="10" group="7961890" id1="327818010" id2="327818010" size="4" type="latdec.dst">38</field>
                <field count="0" flags="0" format="10" group="7961890" id1="327818011" id2="327818011" size="4" type="longdec.dst">-97</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818012" id2="327818012" size="22" type="org.dst">Level 3
Communications</field>
                <field count="0" flags="0" format="4" group="7961890" id1="327818013" id2="327818013" size="2" type="vlan">9</field>
                <field count="0" flags="0" format="6" group="7961890" id1="327818014" id2="327818014" size="4" type="asn.dst">3356</field>
                <field count="0" flags="0" format="65" group="7961890" id1="327818015" id2="327818015" size="20" type="did">cso-decoder-s3-sm-12</field>
                <field count="0" flags="0" format="8" group="7961890" id1="327818016" id2="327818016" size="8" type="rid">7961890</field>
        </results>
</response>
[root@Concentrator10.25.53.20 ~]#
```

Note1: if your session have more than 500 meta values, you should adjust size value accordingly.
Note2: one can change force-content-type=application/json to output meta value list for the session to JSON format.

REST SDK how to example: how to get pcap for TIME query and how to get meta values for any particular session range on a decoder:
Note: on a decoder, one can ONLY do query on TIME for a decoder since decoder index on TIME only!

1) Use **REST /sdk/query** on time range to get sessionids for sessions captured on the decoder during that time range (below: 12/10/2012 8:00:00 – 12/10/2012 8:01:00):

```
[root@Decoder10.25.53.12 ~]# curl --user 'admin:netwitness' 'http://10.25.53.12:50104/sdk?msg=query&query=select+sessionid+where+time%3D%272012-Dec-10+08%3A00%3A00%27-%272012-Dec-10+08%3A01%3A00%27&force-content-type=text/plain&size=10'
[id1=752249494  id2=1386346137
id1=752249214  id2=752249214  count=0  format=8  value=19823002  type=sessionid  flags=0  group=19823002
id1=752249245  id2=752249245  count=0  format=8  value=19823003  type=sessionid  flags=0  group=19823003
id1=752249276  id2=752249276  count=0  format=8  value=19823004  type=sessionid  flags=0  group=19823004
id1=752249294  id2=752249294  count=0  format=8  value=19823005  type=sessionid  flags=0  group=19823005
id1=752249323  id2=752249323  count=0  format=8  value=19823006  type=sessionid  flags=0  group=19823006
id1=752249368  id2=752249368  count=0  format=8  value=19823007  type=sessionid  flags=0  group=19823007
id1=752249398  id2=752249398  count=0  format=8  value=19823008  type=sessionid  flags=0  group=19823008
id1=752249434  id2=752249434  count=0  format=8  value=19823009  type=sessionid  flags=0  group=19823009
id1=752249457  id2=752249457  count=0  format=8  value=19823010  type=sessionid  flags=0  group=19823010
id1=752249493  id2=752249493  count=0  format=8  value=19823011  type=sessionid  flags=0  group=19823011
]
```

NOTE: query into ip.src=10.25.50.68 on a DECODER wil NOT work below since decoder ONLY index on TIME!

```
[root@Decoder10.25.53.12 ~]# curl --user 'admin:netwitness' 'http://10.25.53.12:50104/sdk?msg=query&query=select+sessionid+where+time%3D%272012-Dec-10+08%3A00%3A00%27-%272012-Dec-10+08%3A01%3A00%27%26%26ip.src%3D10.25.50.68&force-content-type=text/plain&size=10'
[id1=1388581684  id2=1388581683
]
[root@Decoder10.25.53.12 ~]#
```

2) Use **REST /sdk/packets** to extract raw session data into pcap from sessionid range returned above:

```
[root@Decoder10.25.53.12 ~]# curl --user 'admin:netwitness' 'http://10.25.53.12:50104/sdk/packets?&sessions=19823002-19823011' > test.pcap
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 25807    0 25807    0     0   143k      0 --:--:-- --:--:-- --:--:-- 2788k
[root@Decoder10.25.53.12 ~]# ll test.pcap
-rw-r--r-- 1 root root 25807 Dec 14 15:46 test.pcap
```

3) Use **REST /sdk/session** to get metaid range for above sessionid range (field1 and field2 below):

```
[root@Decoder10.25.53.12 ~]# curl --user 'admin:netwitness' 'http://10.25.53.12:50104/sdk?msg=session&id2=19823011&id1=19823002&&force-content-type=text/plain'
id1: 19823002
id2: 19823011
field1: 752249214
field2: 752249520
```

4) Use **REST /sdk/query** to extract all meta values from the metaid range returned above:
Note1: adjust size value below accordingly if you have large meta value outputs (note in above example, total meta values is **306** = 752249520 – 792249214).
Note2: one can change force-content-type=application/json to output meta value list for the session to JSON format below.

```
[root@Decoder10.25.53.12 ~]# curl --user "admin:netwitness" 'http://10.25.53.12:50104/sdk?msg=query&force-content-type=text/xml&id1=752249214&id2=752249520&query=select%20*&size=500' > metalist.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 40925  100 40925    0     0  2698k      0 --:--:-- --:--:-- --:--:-- 23.5M
[root@Decoder10.25.53.12 ~]# cat metalist.txt
<?xml version="1.0" encoding="utf-8"?>
```

<response flags="1074200577">
<results id1="752249521" id2="752249520">
<field count="0" flags="0" format="8" group="19823002" id1="752249214" id2="752249214" size="8" type="sessionid">19823002</field>
<field count="0" flags="0" format="32" group="19823002" id1="752249215" id2="752249215" size="8" type="time">1355126400</field>
<field count="0" flags="0" format="6" group="19823002" id1="752249216" id2="752249216" size="4" type="size">134</field>
<field count="0" flags="0" format="6" group="19823002" id1="752249217" id2="752249217" size="4" type="payload">0</field>
<field count="0" flags="0" format="2" group="19823002" id1="752249218" id2="752249218" size="1" type="medium">1</field>
…… (omitted, note group= is the sessionid for the meta value) ……
<field count="0" flags="0" format="2" group="19823011" id1="752249505" id2="752249505" size="1" type="ip.proto">6</field>
<field count="0" flags="0" format="2" group="19823011" id1="752249506" id2="752249506" size="1" type="tcp.flags">27</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249507" id2="752249507" size="9" type="risk.info">flags_fin</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249508" id2="752249508" size="9" type="risk.info">flags_syn</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249509" id2="752249509" size="9" type="risk.info">flags_psh</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249510" id2="752249510" size="9" type="risk.info">flags_ack</field>
<field count="0" flags="0" format="4" group="19823011" id1="752249511" id2="752249511" size="2" type="tcp.srcport">40552</field>
<field count="0" flags="0" format="4" group="19823011" id1="752249512" id2="752249512" size="2" type="tcp.dstport">2012</field>
<field count="0" flags="0" format="6" group="19823011" id1="752249513" id2="752249513" size="4" type="service">22</field>
<field count="0" flags="0" format="2" group="19823011" id1="752249514" id2="752249514" size="1" type="streams">2</field>
<field count="0" flags="0" format="6" group="19823011" id1="752249515" id2="752249515" size="4" type="packets">88</field>
<field count="0" flags="0" format="4" group="19823011" id1="752249516" id2="752249516" size="2" type="lifetime">1</field>
<field count="0" flags="0" format="6" group="19823011" id1="752249517" id2="752249517" size="4" type="rpackets">28</field>
<field count="0" flags="0" format="6" group="19823011" id1="752249518" id2="752249518" size="4" type="rpayload">4688</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249519" id2="752249519" size="10" type="crypto">aes128-ctr</field>
<field count="0" flags="0" format="65" group="19823011" id1="752249520" id2="752249520" size="10" type="alert">John-Test1</field>
</results>
</response>
[root@Decoder10.25.53.12 ~]#