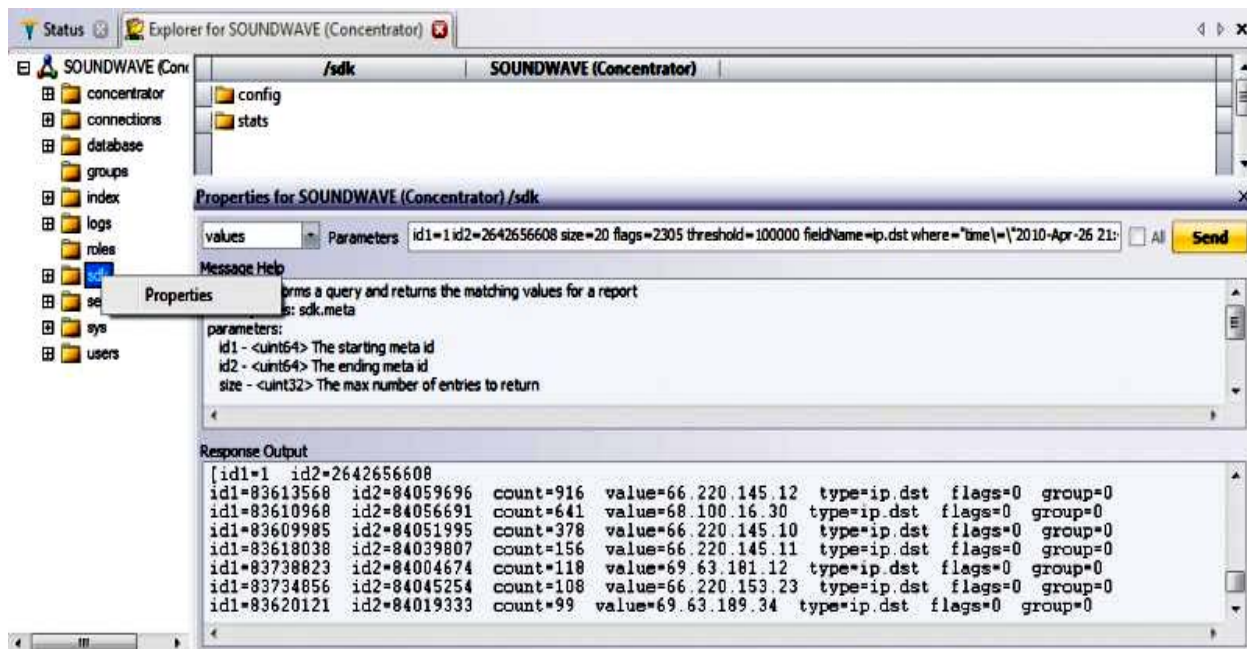


Below is a picture of running a SDK values call from Administrator's Explorer View. Open up explorer on the service of interest, select the /sdk node and right click and choose properties. The properties dialog will appear where you can select and run all supported messages on that node.

The /sdk node is where all the query functionality is contained. Using the log messages I posted above, I selected the full text of the query and submitted it to the "values" message for the IP Destination report. You can tell from the audit log that I ran a values call because it says "issued values". If it said "issued query", then you would select the query message, etc.



From the output, you can see some of the destination IP addresses for www.facebook.com.

This shows how you can submit and view results from the exact query in an audit log.

If you wanted to see the results from NwConsole, use the "login" command and then submit the query like this:

```
[root@SOUNDWAVE ~]# NwConsole
```

```
NetWitness Console 9.0.5.4
```

```
Copyright 2001-2009, NetWitness Corporation. All Rights Reserved.
```

```
> login localhost:50005 admin netwitness 1
```

```
Successfully logged in as session 5348435
```

```
[localhost:50005] /> /sdk values id1=1 id2=2642656608 size=20 flags=2305 threshold=100000 fieldName=ip.dst where="time"=\'2010-Apr-26 21:47:16\'-\'2010-Apr-27 21:47:15\'" && alias.host=\'www.facebook.com\'"
```

```
[id1=1 id2=2642656608
```

```
id1=83613568 id2=84059696 count=916 value=66.220.145.12 type=ip.dst flags=0 group=0
```

```
id1=83610968 id2=84056691 count=641 value=68.100.16.30 type=ip.dst flags=0 group=0
```

```
id1=83609985 id2=84051995 count=378 value=66.220.145.10 type=ip.dst flags=0 group=0
```

```
id1=83618038 id2=84039807 count=156 value=66.220.145.11 type=ip.dst flags=0 group=0
```

```
id1=83738823 id2=84004674 count=118 value=69.63.181.12 type=ip.dst flags=0 group=0
```