Background:
These tests were performed to understand the effects of shortening the active-timeout and idle-timeout settings in the yaf.conf file and changing the FLUSH_TIMEOUT settings in the rwflowpack.conf file would provide near real-time flow readings.
The test was run on a laptop with SiLK running in a virtual environment. A single pcap was played using tcpreplay with a validation script, based on scapy as a second reference point.

Yaf: conf
YAF_EXTRAFLAGS="-d --live pcap --in eth1 --ipfix tcp --out 127.0.0.1 --ipfix-port 18001 --log /home/mdir/run/log/yaf.log --loglevel=warning --silk --active-timeout=30 --idle-timeout=30 --force-read-all --applabel --live=pcap --max-payload=2048 --mac sourceMacaddress destinationMacaddress --plugin-name=/usr/local/lib/yaf/dpacketplugin.la --pidfile /home/mdir/run/pid/yaf.pid"

Rwflowpack.conf
FLUSH_TIMEOUT=30

rc.sh
#!/bin/bash
rwfilter --start-date=2015/12/10 --stime=2015/12/10:00:00:00-2015/12/10:23:59:59 --type=all --print-volume-statistics --any-address=x.x.x.x --pass-destination=stdout | rwcount --bin-size=3600

```
     |                Recs|             Packets|               Bytes|      Files|
Total|                 214|                4736|             3802923|          1|
 Pass|                 214|                4736|             3802923|           |
 Fail|                   0|                   0|                   0|           |
                 Date|         Records|               Bytes|           Packets|
2015/12/10T12:00:00|          214.00|          3802923.00|           4736.00|
```

tcpreplay output (which was used to play the pcap)

```
sending out eth1
processing file: http.pcap
Actual: 4767 packets (3880464 bytes) sent in 131.35 seconds.          Rated: 29542.9 bps, 0.23 Mbps, 36.29 pps
Statistics for network device: eth1
        Attempted packets:         4767
        Successful packets:        4767
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

Scapy-based script last line of output (to validate the count of packets, #packetcount@time->packet summary):
#4767@2015-12-10:12:38:13->Ether / IP / TCP 199.59.148.20:http > 192.168.2.76:52113 A

Summary Observation:

	Count of packets	Count of bytes
tcpreplay	4767	3880464
rwfilter | rwcount	4736	3802923

Q1: SiLK reports fewer bytes. Is this because yaf consumes only 2048 bytes of each packet payload and discards the rest, thus lowering the byte count reported?
Q2: SiLK reports fewer packets than what tcpreplay and the script report. The latter two are indentical—4767 packets. What could be the reason for this?

>> Changed yaf and rwflowpack settings and restarted these processes.

Yaf.conf
YAF_EXTRAFLAGS="-d --live pcap --in eth1 --ipfix tcp --out 127.0.0.1 --ipfix-port 18001 --log /home/mdir/run/log/yaf.log --loglevel=warning --silk --active-timeout=3600 --idle-timeout=600 --force-read-all --applabel --live=pcap --max-payload=2048 --mac sourceMacaddress destinationMacaddress --plugin-name=/usr/local/lib/yaf/dpacketplugin.la --pidfile /home/me/run/pid/yaf.pid"

Rwflowpack.conf
FLUSH_TIMEOUT=3600

rc.sh
#!/bin/bash
rwfilter --start-date=2015/12/10 --stime=2015/12/10:13:30:00-2015/12/10:23:59:59 --type=all --print-volume-statistics --any-address=x.x.x.x --pass-destination=stdout | rwcount --bin-size=3600

```
     |                Recs|             Packets|               Bytes|      Files|
Total|                 420|                9534|             7627452|          2|
 Pass|                 194|                4767|             3813726|           |
 Fail|                 226|                4767|             3813726|           |
                  Date|         Records|                Bytes|           Packets|
2015/12/10T13:00:00|          194.00|          3813726.00|           4767.00|
```

tcpreplay

```
sending out eth1
processing file: http.pcap
Actual: 4767 packets (3880464 bytes) sent in 131.50 seconds.          Rated: 29509.2 bps, 0.23 Mbps, 36.25 pps
Statistics for network device: eth1
        Attempted packets:         4767
        Successful packets:        4767
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
incisor@Inx:/media/sf_Share/pca/bro-pcaps$
```

Script:
#1@2015-12-10:13:45:30->Ether / IP / TCP 208.85.42.28:http > 192.168.2.76:52025 A / Raw
#4767@2015-12-10:13:47:42->Ether / IP / TCP 199.59.148.20:http > 192.168.2.76:52113 A

Summary Observation:

	Count of packets	Count of bytes
tcpreplay	4767	3880464
rwfilter | rwcount	4767	3813726

Q3: Q2 appears to be answered with this run. Is the reason that the packet counts are now matched because the SiLK processes (yaf and rwflowpack) were bounced causing more buffers to be flushed to the disk?
Q4: The count of records fewer the second time the identical pcap was played? 226 the first time, and 194 the second time. Is my assumption correct that this is because the longer active timeout has caused fewer but denser flows?