

```
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i1 (vpn decrypt)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i2 (Stateless verifications)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:i[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i4 (vpn decrypt)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:I[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i5 (SecureXL inbound)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:o[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i6 (SecureXL inbound)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:O[60]: 10.2.254.2 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o5 (vpn polic outbound)[84]: 172.16.1.1 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O5 (SecureXL outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O6 (vpn encrypt)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.1 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[52]: 172.16.1.3 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S....A. seq=5c2282fb ack=5c3b9466
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o1 (vpn nat outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o3 (fw VM outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o2 (Stateless verifications)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
```

Implementing an IDS Solution with Challenges: Budget, Significant Traffic, Correlation, and Limited Resources

RAID 2005

**Russ McRee
Poster Session**

The Challenges

- Budget

- Significant Traffic

- Correlation

- Limited Resources

```
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i1 (vpn decrypt)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i2 (Stateless verifications)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:I[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:o[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:I8 (IP Options Restore)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:O[60]: 10.2.254.2 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O4 (vpn nat outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S. A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 10.2.254.2 -> 10.2.254.2 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O5 (SecureXL outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O6 (vpn encrypt)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[52]: 172.16.1.3 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S. A. seq=5c2282fb ack=5c3b9466
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o1 (vpn nat outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o3 (fw VM outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:o[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:o2 (Stateless verifications)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S. .... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
```

Budget

- Government entity budget

(we don't have any)

- Open source makes Finance

Directors happy

- Open source tools can perform

as well as their commercial

(expensive) counterparts

Significant traffic

- Part of a larger network

- Fat fiber backbone, multiple ISPs

- Tons of noise from departmental neighbors

- Flat network, not enough use of isolated networks

Correlation

- Behind the firewall of large organization divided into many departments
- Without network separation and departmental firewalls, much neighborhood traffic requires suppression
- False positives? Does suppression lead to false negatives?
- - SNMP/ICMP by the pound
- - What is a real attack?

Limited Resources

- Government entity staffing

(we don't have any)

- Who analyzes? Me

- Who receives alerts? Me

- Who takes the fall when it all goes to hell? Me

Snort, Apache, SSL, PHP, MySQL, and ACID/BASE

- Great packages but usually built around Red Hat/Fedora (distros require a great deal of hardening)
- ACID/BASE really bog down around 250,000 events
- Requires much care & feeding

OSSIM

Open Source Security Information Manager

- Still maturing
- A bit convoluted, very slow
- PHP dependent
- Troublesome configuring graphing and sensors
- Trying to be all things to all people (Snort, Acid, Mrtg, NTOP, OpenNMS, nmap, nessus)

Sguil

- Recommended OS: FreeBSD

- A true analyst's console

- Not browser based

- Very promising, but difficult to install

- Also still maturing, but under constant development

Sguil offers:

- Real time results

- Comprehensive query capacity

- Fast!

- Superior correlation, escalation, alert categorization, and workflow

AANVAL

- Also requires Snort, Apache, PHP, and MySQL
- A happy medium between Sguil and ACID/BASE installations
- Easy to install
- Commercial version and support available
- More mature, more rapid development thanks to commercial product offering
- Also slows down, like ACID/BASE, after 250,000 +/- events, but is faster

AANVAL offers:

- Correlation
- Excellent graphing
- Easy installation
- Strong reporting tools
- Scalable
- Can manage Snort sensors as well as syslog feeds

```
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i1 (vpn decrypt)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i2 (Stateless verifications)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:i[60]: 172.16.1.1 -> 172.16.1.3 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:I[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:i3 (vpn decrypt verify)[84]: 172.16.1.1 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:O[60]: 172.16.1.1 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=8 code=0 echo request id=16436 seq=256 ICMP: type=8 code=0 echo request id=16436 seq=256
eth0:I8 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.2 (ICMP) len=84 id=11936
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:O[60]: 10.2.254.2 -> 10.2.4.12 (TCP) len=60 id=46125
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O4 (vpn policy outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb TCP: 80 -> 34838 .S..A. seq=5c3b9465 ack=5c2282fb
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:i[52]: 10.2.4.12 -> 10.2.254.2 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O5 (Seq. number restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O6 (vpn encrypt)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[52]: 10.2.4.12 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[52]: 172.16.1.3 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O7 (IP Options Restore)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466 TCP: 34838 -> 80 .S..A. seq=5c2282fb ack=5c3b9466
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[52]: 172.16.1.3 -> 172.16.1.1 (TCP) len=52 id=46126
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O1 (vpn decrypt)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth1:I[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O3 (fw VNI outbound)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 10.2.4.12 -> 172.16.1.1 (TCP) len=60 id=46124
ICMP: type=0 code=0 echo reply id=16436 seq=256 ICMP: type=0 code=0 echo reply id=16436 seq=256
eth0:O2 (Stateless verifications)[84]: 172.16.1.2 -> 172.16.1.1 (ICMP) len=84 id=49943
TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000 TCP: 34838 -> 80 .S.... seq=5c2282fa ack=00000000
[6b770000 - 3e5c776b 00000000 020110ac 000007b6]:eth0:O[60]: 172.16.1.3 -> 172.16.1.1 (TCP) len=60 id=46124
```

Conclusion

- For those facing the classic challenges including budget, significant traffic, correlation, and limited resources, AANVAL appears to offer a free or low cost solution that includes all of the benefits of ACID/BASE with a better, faster interface
- AANVAL in concert with Sguil appear to be a viable toolset