WIRESHARK

JUST HTTP

NOT THIS AND NOT THAT AND NOT THAT EITHER

```
!( tcp.port == 389) and !( tcp.port == 11211) and !( tcp.port == 1521) and
!ssh and !dlm3 and !(ip.src == 139.230.244.128) and !(ip.src == 10.67.124.6)
and !(ip.dst == 10.67.124.6)
```

NOT ME OR APP SWITCH

```
tcp.port == 80 and !(ip.dst == 10.31.66.91) and !(ip.src == 10.31.66.91) and
!(ip.src == 10.67.124.6) and !(ip.dst == 10.67.124.6) and !(ip.src ==
10.67.124.8) and !(ip.dst == 10.67.124.8)
```

NOT PORT X

```
!( tcp.port == 1521)
```

APP SWITCH CONNECTIONS - DEPENDS ON CAMPUS LOCATION OF REAL SERVER

```
http and ip.dst == 10.1.122.0/24 and ip.src == 10.1.122.0/24
http and ip.dst == 10.67.124.0/24 and ip.src == 10.67.124.0/24
```

HD8001090 HTTP

```
ip.src == 10.31.66.91 or ip.dst == 10.31.66.91 and http
```

QA EXCLUDING MONITORING

```
http and ip.dst != 139.230.244.129 and ip.src != 139.230.244.129 and ip.dst
!= 139.230.80.11 and ip.src != 139.230.80.11
```

DUMP ETH0 REQUESTS

```
# tcpdump -nnvvXSs 0 -i eth0 tcp -w /tmp/`hostname`_tcpdump_`date +%Y-%m-
%dT%H-%M-%S`.pcap
```

DUMP LOCAL REQUESTS

```
# tcpdump -nnvvXSs 0 -i lo tcp and src 10.1.122.131 -w
/tmp/`hostname`_tcpdump_`date +%Y-%m-%dT%H-%M-%S`.pcap
```

DUMP ETH0 REQUESTS FROM IP RANGE

```
# tcpdump -nnvvXSs 0 -i eth0 tcp and src net 10.31.71.0/24 -w
/app/wcms.ecu/tmp/`hostname`_tcpdump_`date +%Y-%m-%dT%H-%M-%S`.pcap
```

DUMP SNMP MONITOR SESSION - NOTE: FILENAME EXT IS IMPORTANT FOR WIRESHARK ON WINDOWS

```
# tcpdump -nnvvXSs 0 tcp and dst 139.230.80.11 -w
/app/wcms.ecu/tmp/`hostname`_tcpdump_`date +%Y-%m-%dT%H-%M-%S`.pcap
# tcpdump -nnvvXSs 0 tcp and src 10.1.122.6 -w
/app/wcms.ecu/tmp/`hostname`_tcpdump_`date +%Y-%m-%dT%H-%M-%S`.pcap
# tcpdump -nnvvXSs 0 tcp and dst 10.1.122.8 -w
/app/wcms.ecu/tmp/`hostname`_tcpdump_`date +%Y-%m-%dT%H-%M-%S`.pcap
```