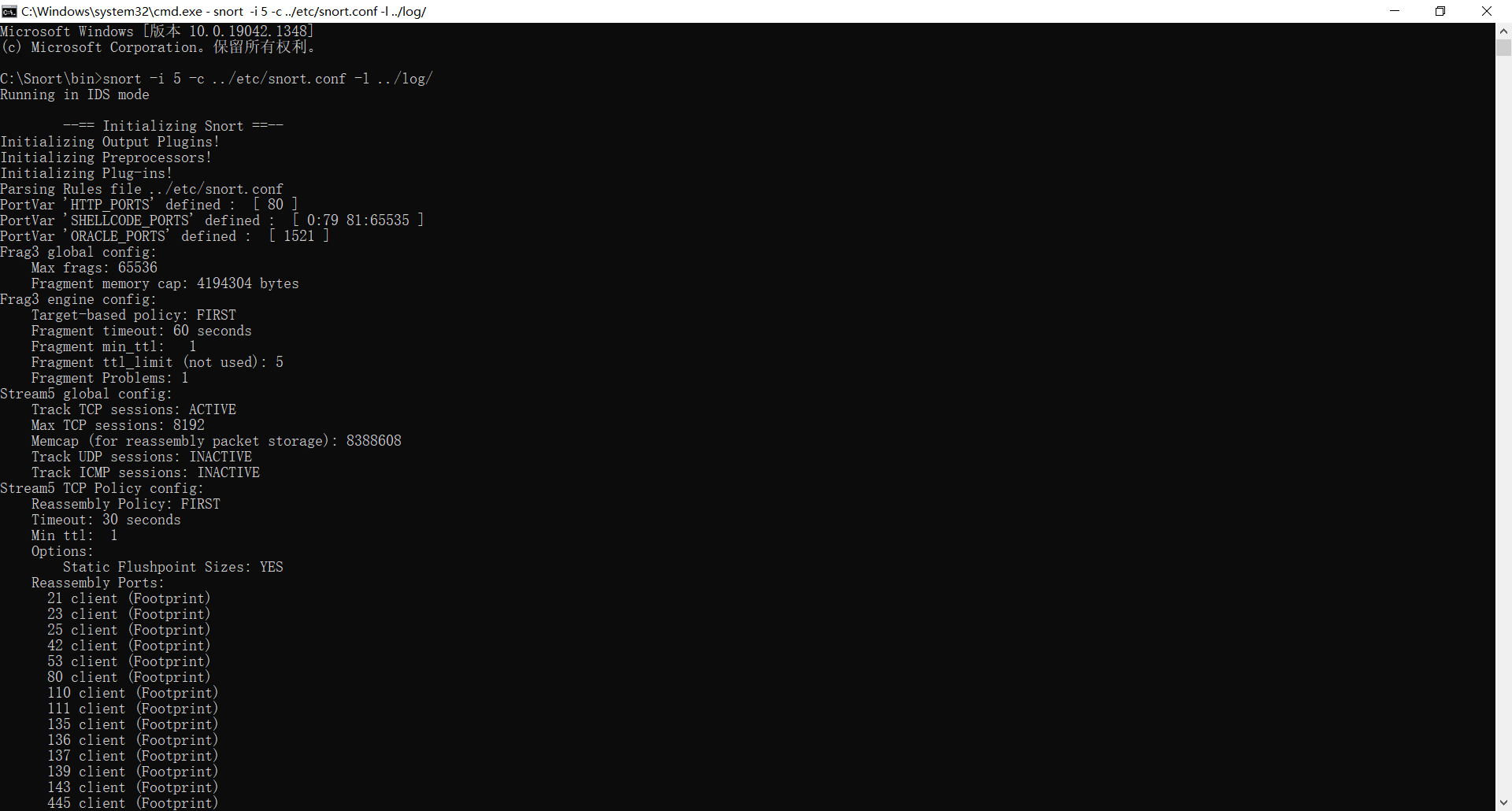
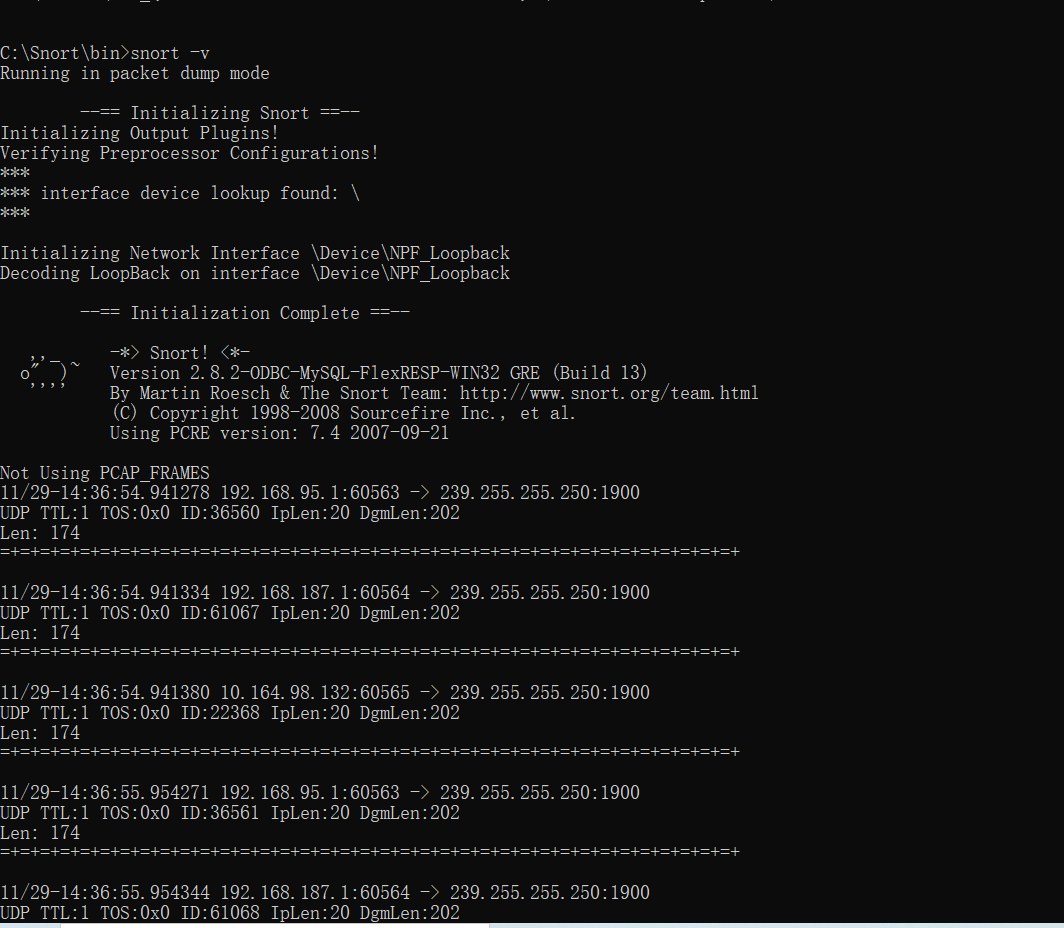


snort –i 5 –c ../etc/snort.conf –l ../log/



snort -v



**snort -c ../etc/snort.conf -l ../log -h 192.168.1.0/24**

./snort -c snort.conf -h 192.168.1.0/24

snort -c snort.conf -l ./log -s -h 192.168.1.0/24

-c是配置文件，-i是接口，-l是存放日志的位置. 使用-s选项可以使snort把报警消息发送到syslog，默认的设备是LOG\_AUTHPRIV和LOG\_ALERT。可以修改snort.conf文件修改其配置。

编写snort 规则(.rule文件):snort使用一种简单的，轻量级的规则描述语言，这种语言灵活而强大。在开发snort规则时要记住几个简单的原则。