alert ip any any -> 121.128.196.0/24 any (content-list₩"BOB"; msg: "BOB word was detected";)

-Alert? Rule will generate an alert message when criteria met

-From any source IP, any port number to 121.128.196.0 ~ 121.128.196.255 with any port

-a text file named "BOB" which contains a list of strings to be searched
 ex) "assignments", "quiz", "Niko"

-search strings in the data portion of packets, then gives us msg;
 "BOB word was detected"

Snort Rules_BOB6 Digital Forensic Track_ 정해원 교육생