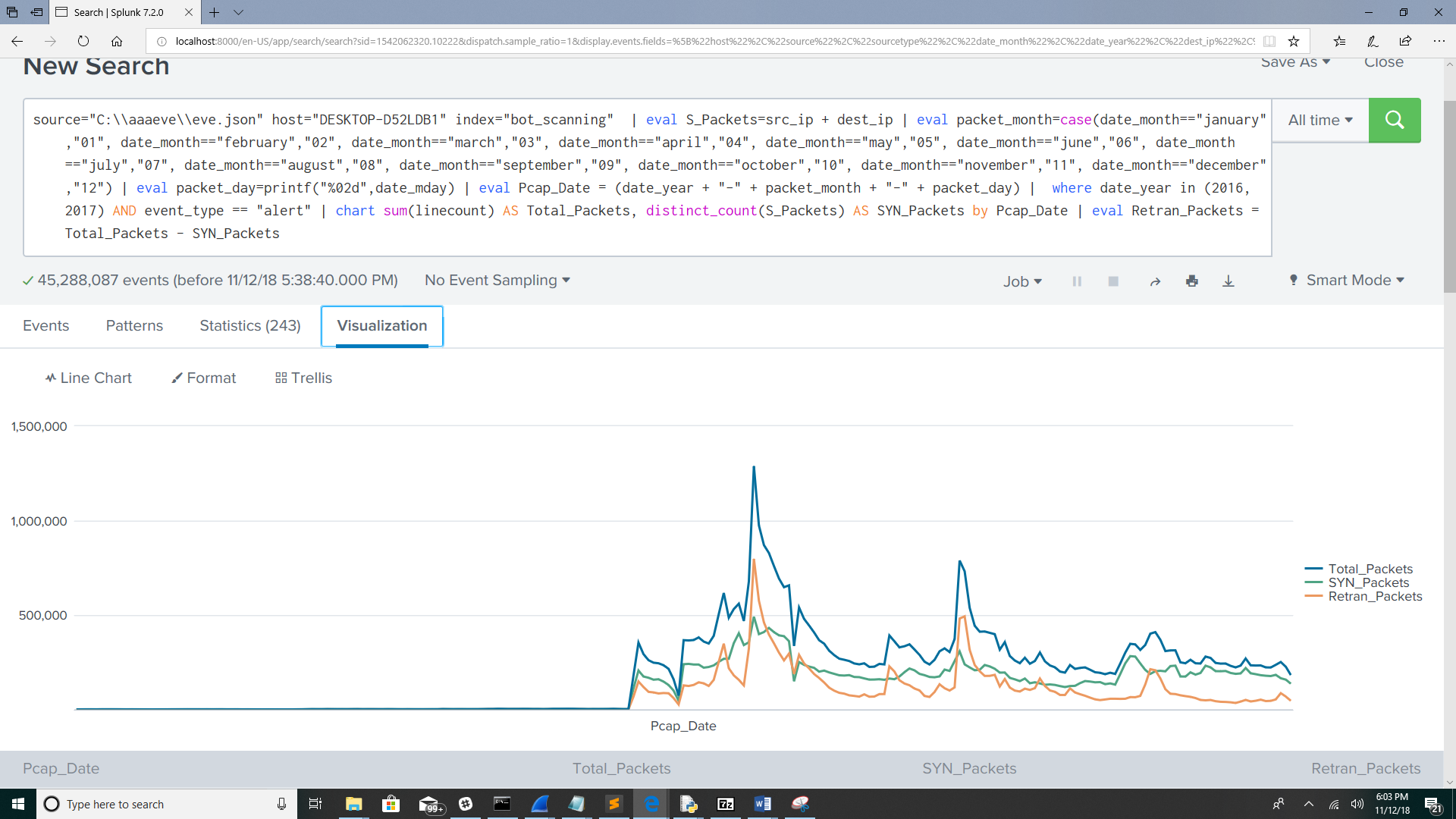
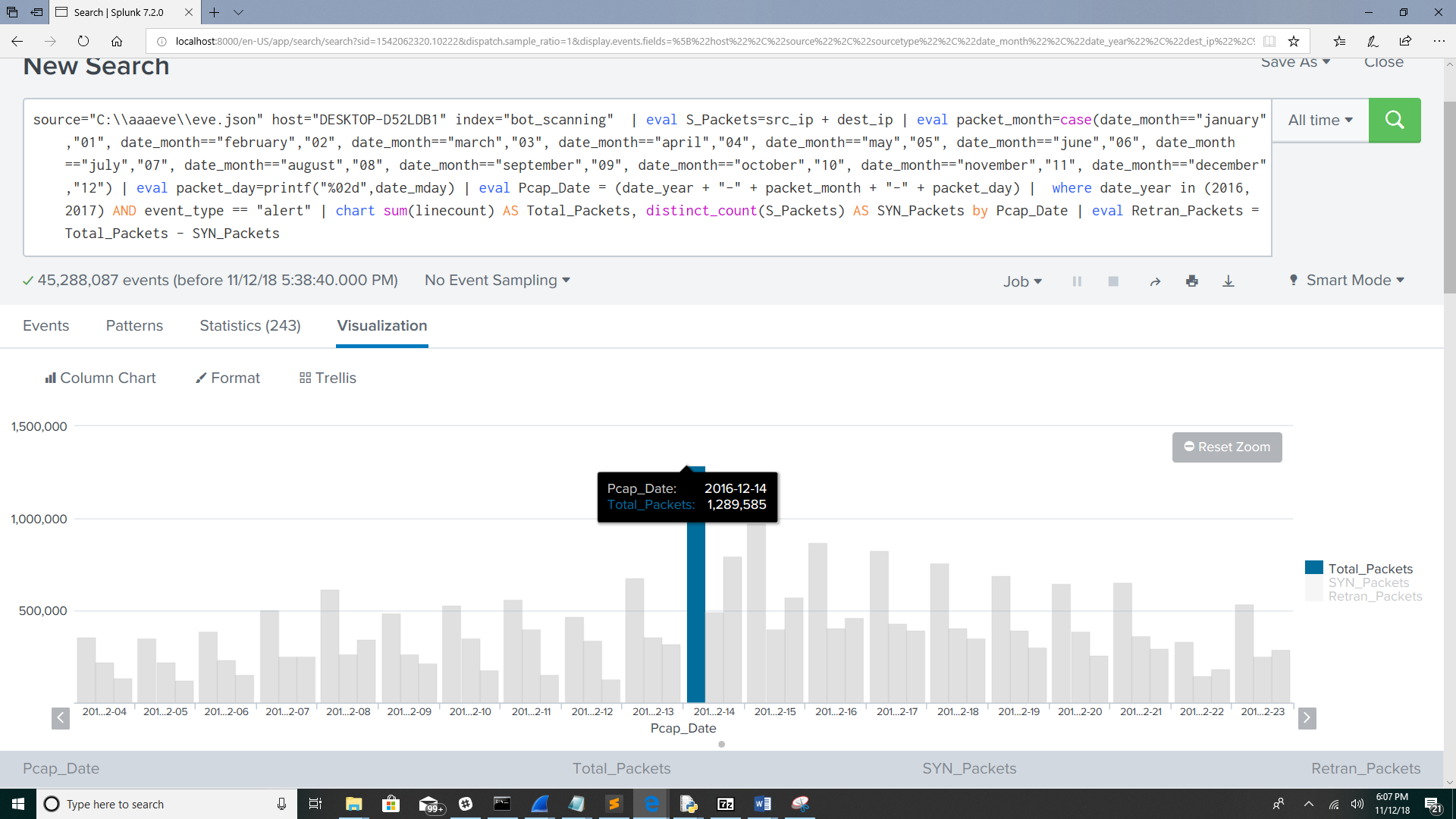
Packet totals

source="C:\\aaaeve\\eve.json" host="DESKTOP-D52LDB1" index="bot\_scanning" | eval S\_Packets=src\_ip + dest\_ip | eval packet\_month=case(date\_month=="january","01", date\_month=="february","02", date\_month=="march","03", date\_month=="april","04", date\_month=="may","05", date\_month=="june","06", date\_month=="july","07", date\_month=="august","08", date\_month=="september","09", date\_month=="october","10", date\_month=="november","11", date\_month=="december","12") | eval packet\_day=printf("%02d",date\_mday) | eval Pcap\_Date = (date\_year + "-" + packet\_month + "-" + packet\_day) | where date\_year in (2016, 2017) AND event\_type == "alert" | chart sum(linecount) AS Total\_Packets, distinct\_count(S\_Packets) AS SYN\_Packets by Pcap\_Date | eval Retran\_Packets = Total\_Packets - SYN\_Packets

<http://localhost:8000/en-US/app/search/search?sid=1542062320.10222>





Bot Totals

source="C:\\aaaeve\\eve.json" host="DESKTOP-D52LDB1" index="bot\_scanning" | eval packet\_month=case(date\_month=="january","01", date\_month=="february","02", date\_month=="march","03", date\_month=="april","04", date\_month=="may","05", date\_month=="june","06", date\_month=="july","07", date\_month=="august","08", date\_month=="september","09", date\_month=="october","10", date\_month=="november","11", date\_month=="december","12") | eval packet\_day=printf("%02d",date\_mday) | eval Pcap\_Date = (date\_year + "-" + packet\_month + "-" + packet\_day) | where date\_year in (2016, 2017) AND event\_type == "alert" | chart distinct\_count(src\_ip) AS Bots, distinct\_count(dest\_ip) AS Pot\_Bot\_Victims by Pcap\_Date

<http://desktop-d52ldb1:8000/en-US/app/search/search?sid=1541973888.3171>

