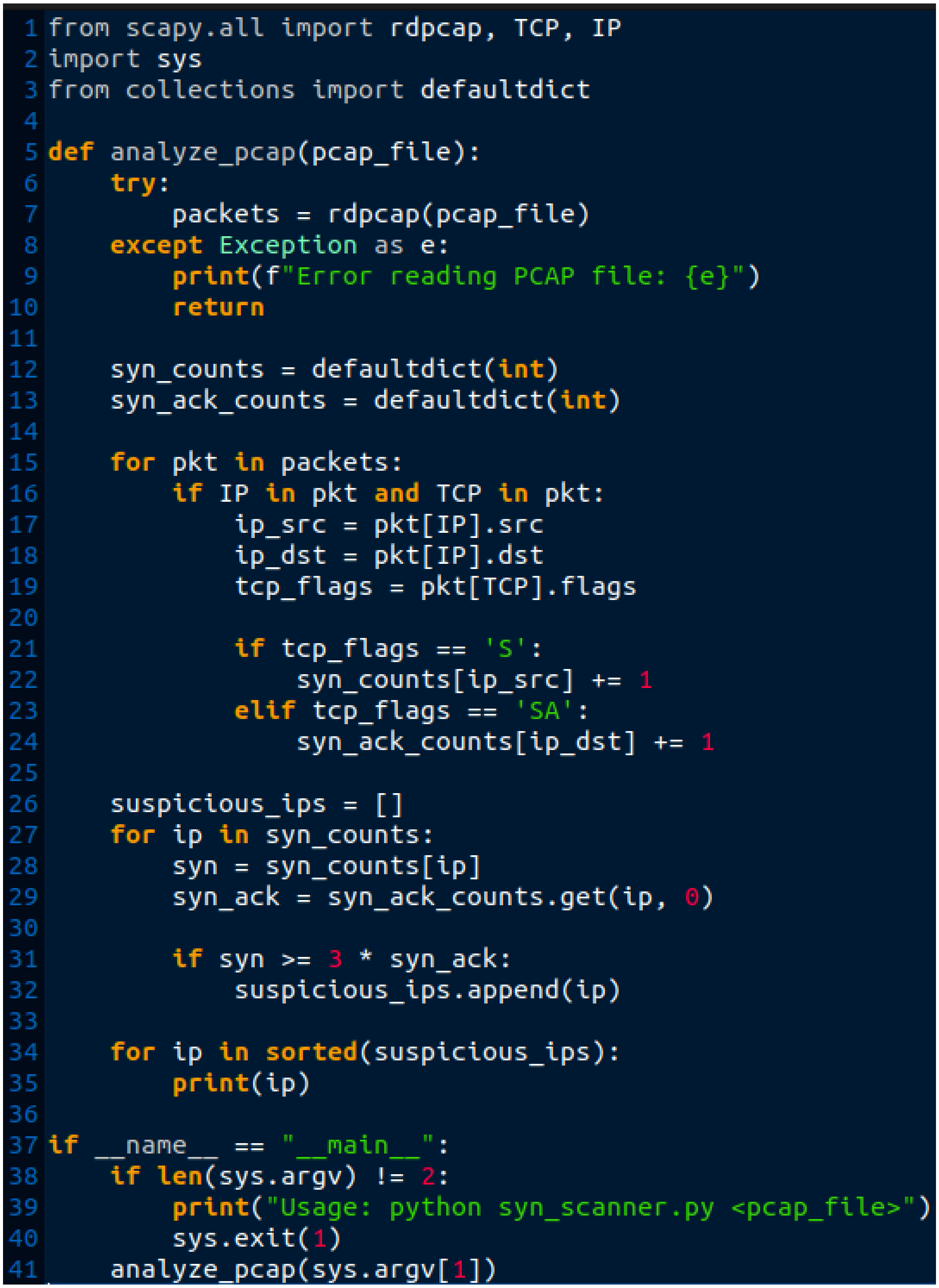
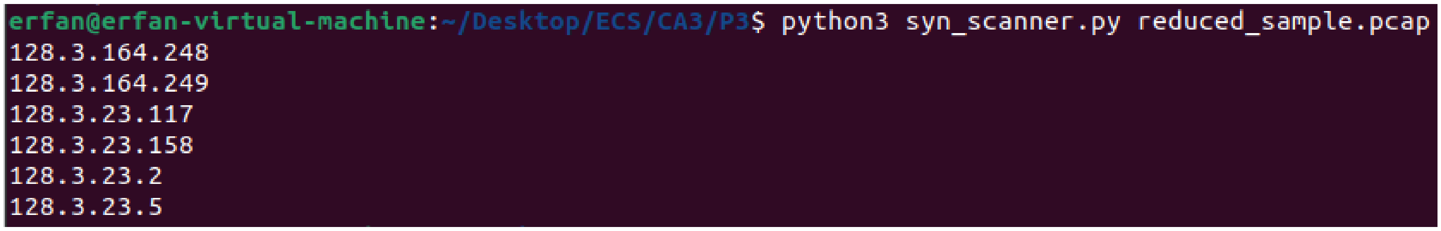


```python
from scapy.all import rdpcap, TCP, IP
import sys
from collections import defaultdict

def analyze_pcap(pcap_file):
    try:
        packets = rdpcap(pcap_file)
    except Exception as e:
        print(f"Error reading PCAP file: {e}")
        return

    syn_counts = defaultdict(int)
    syn_ack_counts = defaultdict(int)

    for pkt in packets:
        if IP in pkt and TCP in pkt:
            ip_src = pkt[IP].src
            ip_dst = pkt[IP].dst
            tcp_flags = pkt[TCP].flags

            if tcp_flags == 'S':
                syn_counts[ip_src] += 1
            elif tcp_flags == 'SA':
                syn_ack_counts[ip_dst] += 1

    suspicious_ips = []
    for ip in syn_counts:
        syn = syn_counts[ip]
        syn_ack = syn_ack_counts.get(ip, 0)

        if syn >= 3 * syn_ack:
            suspicious_ips.append(ip)

    for ip in sorted(suspicious_ips):
        print(ip)

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print("Usage: python syn_scanner.py <pcap_file>")
        sys.exit(1)
    analyze_pcap(sys.argv[1])
```

The script starts by loading the PCAP file and then iterates through each packet, checking if it contains IP and TCP layers. For every packet, it looks for SYN and SYN-ACK. It keeps track of how many SYN packets each IP sends and how many SYN-ACK responses they receive. If an IP sends at least three times more SYN packets than it gets SYN-ACK replies, it’s flagged as suspicious.

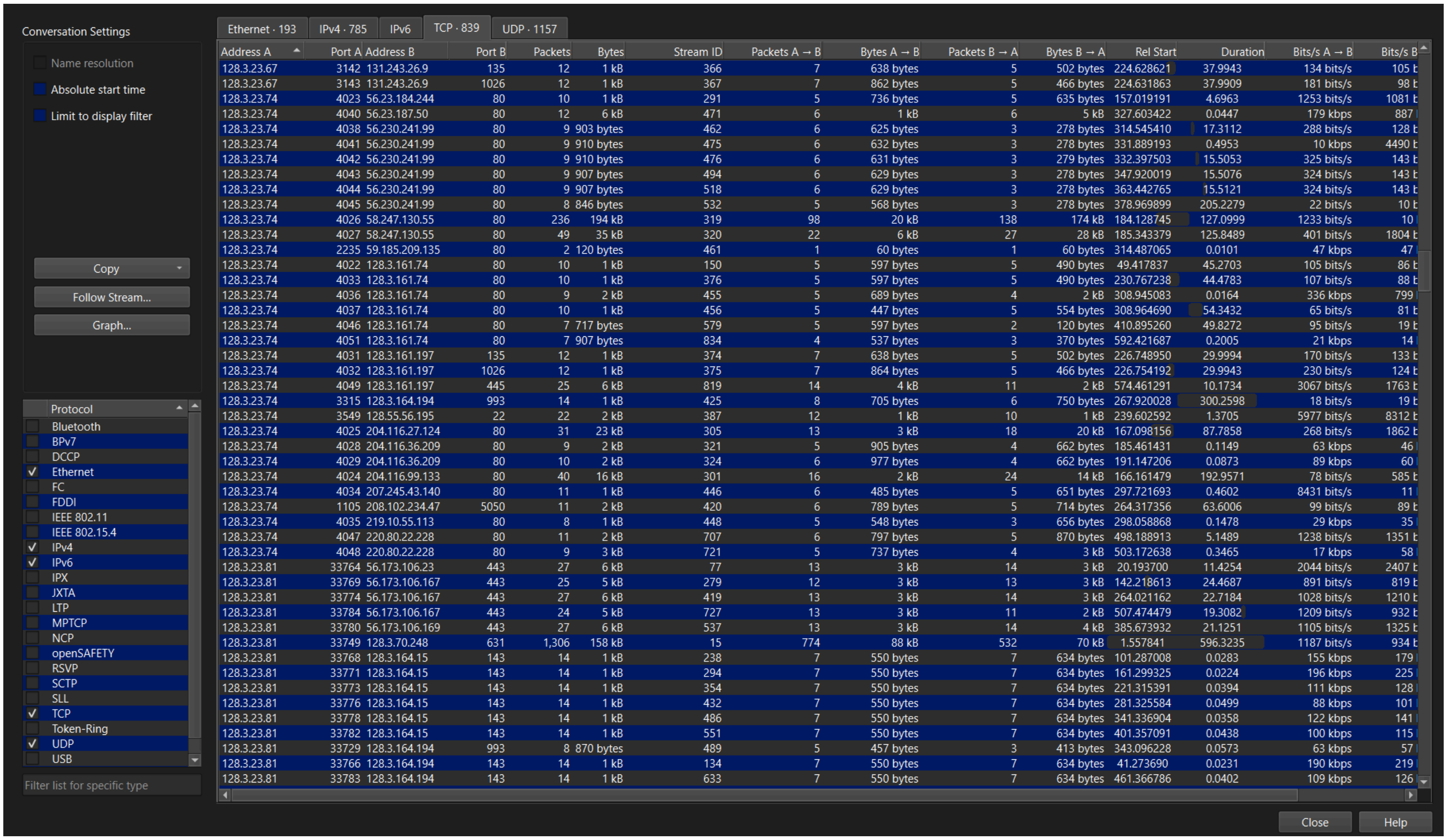


```
erfan@erfan-virtual-machine:~/Desktop/ECS/CA3/P3$ python3 syn_scanner.py reduced_sample.pcap
128.3.164.248
128.3.164.249
128.3.23.117
128.3.23.158
128.3.23.2
128.3.23.5
```

Question:

In the top menu, we select Statistics > Conversations. A new window opens with several tabs. We choose the TCP tab. Here, we can see all TCP connections between pairs of IP addresses and ports. We click the column Address A to sort by the sender IPs. We look for one source IP that appears repeatedly as the initiator with many different destination IPs or ports. If we see one IP with many connections (and especially if these are short conversations with only a few packets each), that is suspicious for scanning or SYN flood.

128.3.23.74 is initiating connections to many IPs/ports (a pattern of a port scan or network scan). Most connections are short-lived (under 15 packets) (probe and move on). It’s not just HTTP (80) or one service (the behavior of a scanner looking for open services). This activity strongly suggests that 128.3.23.74 is performing a network scan.



Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filter

Protocol
☐ Bluetooth
☐ BPv7
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ LTP
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP
☐ SLL
☑ TCP
☐ Token-Ring
☑ UDP
☐ USB

Filter list for specific type

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B
128.3.23.67	3142	131.243.26.9	135	12	1 kB	366	7	638 bytes	5	502 bytes	224.628621	37.9943	134 bits/s	105 b
128.3.23.67	3143	131.243.26.9	1026	12	1 kB	367	7	862 bytes	5	466 bytes	224.631863	37.9909	181 bits/s	98 b
128.3.23.74	4023	56.23.184.244	80	10	1 kB	291	5	736 bytes	5	635 bytes	157.019191	4.6963	1253 bits/s	1081 b
128.3.23.74	4040	56.23.187.50	80	12	6 kB	471	6	1 kB	6	5 kB	327.603422	0.0447	179 kbps	887
128.3.23.74	4038	56.230.241.99	80	9	903 bytes	462	6	625 bytes	3	278 bytes	314.545410	17.3112	288 bits/s	128 b
128.3.23.74	4041	56.230.241.99	80	9	910 bytes	475	6	632 bytes	3	278 bytes	331.889193	0.4953	10 kbps	4490 b
128.3.23.74	4042	56.230.241.99	80	9	910 bytes	476	6	631 bytes	3	279 bytes	332.397503	15.5053	325 bits/s	143 b
128.3.23.74	4043	56.230.241.99	80	9	907 bytes	494	6	629 bytes	3	278 bytes	347.920019	15.5076	324 bits/s	143 b
128.3.23.74	4044	56.230.241.99	80	9	907 bytes	518	6	629 bytes	3	278 bytes	363.442765	15.5121	324 bits/s	143 b
128.3.23.74	4045	56.230.241.99	80	8	846 bytes	532	5	568 bytes	3	278 bytes	378.969899	205.2279	22 bits/s	10 b
128.3.23.74	4026	58.247.130.55	80	236	194 kB	319	98	20 kB	138	174 kB	184.128745	127.0999	1233 bits/s	10
128.3.23.74	4027	58.247.130.55	80	49	35 kB	320	22	6 kB	27	28 kB	185.343379	125.8489	401 bits/s	1804 b
128.3.23.74	2235	59.185.209.135	80	2	120 bytes	461	1	60 bytes	1	60 bytes	314.487065	0.0101	47 kbps	47
128.3.23.74	4022	128.3.161.74	80	10	1 kB	150	5	597 bytes	5	490 bytes	49.417837	45.2703	105 bits/s	86 b
128.3.23.74	4033	128.3.161.74	80	10	1 kB	376	5	597 bytes	5	490 bytes	230.767238	44.4783	107 bits/s	88 b
128.3.23.74	4036	128.3.161.74	80	9	2 kB	455	5	689 bytes	4	2 kB	308.945083	0.0164	336 kbps	799
128.3.23.74	4037	128.3.161.74	80	10	1 kB	456	5	447 bytes	5	554 bytes	308.964690	54.3432	65 bits/s	81 b
128.3.23.74	4046	128.3.161.74	80	7	717 bytes	579	5	597 bytes	2	120 bytes	410.895260	49.8272	95 bits/s	19 b
128.3.23.74	4051	128.3.161.74	80	7	907 bytes	834	4	537 bytes	3	370 bytes	592.421687	0.2005	21 kbps	14
128.3.23.74	4031	128.3.161.197	135	12	1 kB	374	7	638 bytes	5	502 bytes	226.748950	29.9994	170 bits/s	133 b
128.3.23.74	4032	128.3.161.197	1026	12	1 kB	375	7	864 bytes	5	466 bytes	226.754192	29.9943	230 bits/s	124 b
128.3.23.74	4049	128.3.161.197	445	25	6 kB	819	14	4 kB	11	2 kB	574.461291	10.1734	3067 bits/s	1763 b
128.3.23.74	3315	128.3.164.194	993	14	1 kB	425	8	705 bytes	6	750 bytes	267.920028	300.2598	18 bits/s	19 b
128.3.23.74	3549	128.55.56.195	22	22	2 kB	387	12	1 kB	10	1 kB	239.602592	1.3705	5977 bits/s	8312 b
128.3.23.74	4025	204.116.27.124	80	31	23 kB	305	13	3 kB	18	20 kB	167.098156	87.7858	268 bits/s	1862 b
128.3.23.74	4028	204.116.36.209	80	9	2 kB	321	5	905 bytes	4	662 bytes	185.461431	0.1149	63 kbps	46
128.3.23.74	4029	204.116.36.209	80	10	2 kB	324	6	977 bytes	4	662 bytes	191.147206	0.0873	89 kbps	60
128.3.23.74	4024	204.116.99.133	80	40	16 kB	301	16	2 kB	24	14 kB	166.161479	192.9571	78 bits/s	585 b
128.3.23.74	4034	207.245.43.140	80	11	1 kB	446	6	485 bytes	5	651 bytes	297.721693	0.4602	8431 bits/s	11
128.3.23.74	1105	208.102.234.47	5050	11	2 kB	420	6	789 bytes	5	714 bytes	264.317356	63.6006	99 bits/s	89 b
128.3.23.74	4035	219.10.55.113	80	8	1 kB	448	5	548 bytes	3	656 bytes	298.058868	0.1478	29 kbps	35
128.3.23.74	4047	220.80.22.228	80	11	2 kB	707	6	797 bytes	5	870 bytes	498.188913	5.1489	1238 bits/s	1351 b
128.3.23.74	4048	220.80.22.228	80	9	3 kB	721	5	737 bytes	4	3 kB	503.172638	0.3465	17 kbps	58
128.3.23.81	33764	56.173.106.23	443	27	6 kB	77	13	3 kB	14	3 kB	20.193700	11.4254	2044 bits/s	2407 b
128.3.23.81	33769	56.173.106.167	443	25	5 kB	279	12	3 kB	13	3 kB	142.218613	24.4687	891 bits/s	819 b
128.3.23.81	33774	56.173.106.167	443	27	6 kB	419	13	3 kB	14	3 kB	264.021162	22.7184	1028 bits/s	1210 b
128.3.23.81	33784	56.173.106.167	443	24	5 kB	727	13	3 kB	11	2 kB	507.474479	19.3082	1209 bits/s	932 b
128.3.23.81	33780	56.173.106.169	443	27	6 kB	537	13	3 kB	14	4 kB	385.673932	21.1251	1105 bits/s	1325 b
128.3.23.81	33749	128.3.70.248	631	1,306	158 kB	15	774	88 kB	532	70 kB	1.557841	596.3235	1187 bits/s	934 b
128.3.23.81	33768	128.3.164.15	143	14	1 kB	238	7	550 bytes	7	634 bytes	101.287008	0.0283	155 kbps	179
128.3.23.81	33771	128.3.164.15	143	14	1 kB	294	7	550 bytes	7	634 bytes	161.299325	0.0224	196 kbps	225
128.3.23.81	33773	128.3.164.15	143	14	1 kB	354	7	550 bytes	7	634 bytes	221.315391	0.0394	111 kbps	128
128.3.23.81	33776	128.3.164.15	143	14	1 kB	432	7	550 bytes	7	634 bytes	281.325584	0.0499	88 kbps	101
128.3.23.81	33778	128.3.164.15	143	14	1 kB	486	7	550 bytes	7	634 bytes	341.336904	0.0358	122 kbps	141
128.3.23.81	33782	128.3.164.15	143	14	1 kB	551	7	550 bytes	7	634 bytes	401.357091	0.0438	100 kbps	115
128.3.23.81	33729	128.3.164.194	993	8	870 bytes	489	5	457 bytes	3	413 bytes	343.096228	0.0573	63 kbps	57
128.3.23.81	33766	128.3.164.194	143	14	1 kB	134	7	550 bytes	7	634 bytes	41.273690	0.0231	190 kbps	219
128.3.23.81	33783	128.3.164.194	143	14	1 kB	633	7	550 bytes	7	634 bytes	461.366786	0.0402	109 kbps	126