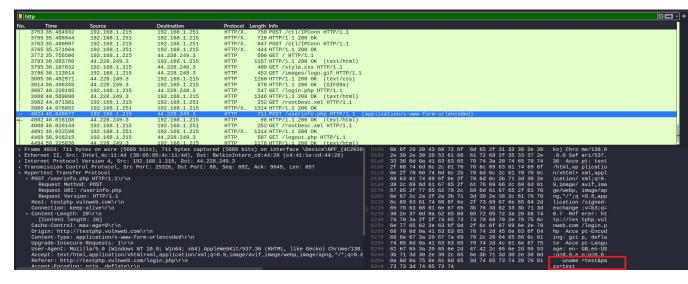
## TASK-1



## TASK-2

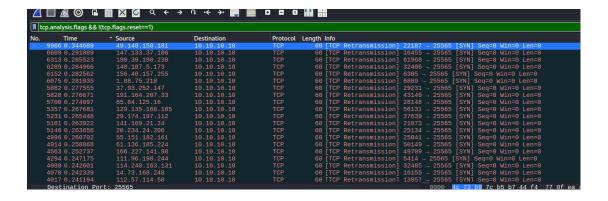
Large numbers of SYN packets were detected from different IP addresses without corresponding SYN+ACK replies.

Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0

	ar Carrier Control	And the second second			
No.	Time	^ Source	Destination	Protocol	Length Info
160	68 0.425906	176.232.188.214	10.10.10.10	TCP	60 12608 → 25565 [SYN] Seq=0 Win=0 Len=0
160	67 0.425906	139.111.37.67	10.10.10.10	TCP	60 26545 → 25565 [SYN] Seq=0 Win=0 Len=0
160	66 0.425905	114.153.32.195	10.10.10.10	TCP	60 20886 → 25565 [SYN] Seq=0 Win=0 Len=0
160	65 0.425904	185.26.176.87	10.10.10.10	TCP	60 46903 → 25565 [SYN] Seq=0 Win=0 Len=0
160	64 0.425838	79.162.213.102	10.10.10.10	TCP	60 9422 → 25565 [SYN] Seq=0 Win=0 Len=0
160	63 0.425837	74.246.255.66	10.10.10.10	TCP	60 56267 → 25565 [SYN] Seq=0 Win=0 Len=0
160	62 0.425837	66.207.81.213	10.10.10.10	TCP	60 9537 → 25565 [SYN] Seq=0 Win=0 Len=0
160	61 0.425836	66.129.151.94	10.10.10.10	TCP	60 40422 → 25565 [SYN] Seq=0 Win=0 Len=0
160	60 0.425835	84.102.177.109	10.10.10.10	TCP	60 5682 → 25565 [SYN] Seq=0 Win=0 Len=0
160	59 0.425835	1.4.242.252	10.10.10.10	TCP	60 59176 → 25565 [SYN] Seq=0 Win=0 Len=0
160	58 0.425767	61.125.211.155	10.10.10.10	TCP	60 40936 → 25565 [SYN] Seq=0 Win=0 Len=0
160	57 0.425767	183.59.70.124	10.10.10.10	TCP	60 63877 → 25565 [SYN] Seq=0 Win=0 Len=0
160	56 0.425766	15.213.165.43	10.10.10.10	TCP	60 38085 → 25565 [SYN] Seq=0 Win=0 Len=0
160	55 0.425766	69.42.177.232	10.10.10.10	TCP	60 63007 → 25565 [SYN] Seq=0 Win=0 Len=0
160	54 0.425687	113.182.96.184	10.10.10.10	TCP	60 23431 → 25565 [SYN] Seq=0 Win=0 Len=0
160	53 0.425686	50.42.102.236	10.10.10.10	TCP	60 46007 → 25565 [SYN] Seq=0 Win=0 Len=0
160	52 0.425686	29.31.136.80	10.10.10.10	TCP	60 53393 → 25565 SYN Seq=0 Win=0 Len=0
160	51 0.425685	58.206.27.214	10.10.10.10	TCP	60 61968 → 25565 SYN Seq=0 Win=0 Len=0
160	50 0.425685	93.101.7.77	10.10.10.10	TCP	60 41226 → 25565 [SYN] Seq=0 Win=0 Len=0
160	49 0.425684	135.104.243.250	10.10.10.10	TCP	60 22412 → 25565 [SYN] Seg=0 Win=0 Len=0

TCP anomalies- TCP Retransmission

Filter: tcp. analysis. flags && !(tcp. flags. reset==1)



CONCLUSION: Detected possible all the SYN packets are from different source IPs, so it's a distributed SYN flood (DDoS) or scanning activity using spoofed source addresses.