***Checklist for intrusion detection in wireshark***

1. Statistics 🡪 Protocol Hierarchy
   1. Can be used to identify protocols that have been used for the transmission.
   2. Can be used to find out what majority of traffic contains.
2. Statistics 🡪 Endpoints
   1. To check the address differences
      1. Ex: A machine that is in Sweden trying to communicate with machine in sri lanka.
   2. Can find pattern between IP addresses
      1. Ex: Set of IP addresses like below means something suspicious activity is going on.  
         192.168.10.7  
         192.168.10.8  
         192.168.10.9  
         192.168.10.10  
         192.168.10.11
3. Statistics 🡪 Conversation
   1. Can use the duration of the conversation to determine whether it is abnormally long.
4. Edit 🡪 Find 🡪 Search for executables
   1. Executables contains a name with random strings ( a random name).
   2. An exe moving from one machine to another is most probably an attack.
5. Right click on any packets 🡪 Follow TCP stream
   1. Can be used to find out whether the responses matches the requests made.
   2. Can be used to identify whether stream contains malicious scripts or encoded messages.
6. If a packet highlighted in red means that a suspicious activity is going on the particular packet.
7. When following the TCP stream if packet contains DNS query that is weirdly long, it means when DNS server runs the query it will crash the DNS server because the query will confuse the DNS server because DNS server doesn’t know what to do for such a long query.
8. Check for strange flag combinations..
   1. A popular attack that uses incorrect flag combination is Christmas tree attack.
9. Check if any fragmentation has occurred,
   1. Fragmentation should be done only if destination’s window size is smaller than the packet size. ( Usually fragmented packets are malicious )
10. Since IPV6 addresses are rarely used, check for use of IPV6 addresses.
    1. IPV6 addresses are widely used for teardrop attacks.
11. There is a range of IP addresses that are known to be malicious. Check whether the IP address is in the malicious range.
12. Check for packets with bad checksum. Packets with bad checksums can be used malicious activity.
13. Check for DNS zone transfers.
14. Check sequence numbers.
15. Check for internal IP addresses coming from the gateway.
16. Check for broadcast addresses.
17. Check Payload.
18. Check for unusual number of ARP requests.
19. Check TTL value.
20. Number of packets that have transferred in conversations.
21. Conversations 🡪 traffic transferred to ports used by standard services
    1. Means that it is a NMAP scan