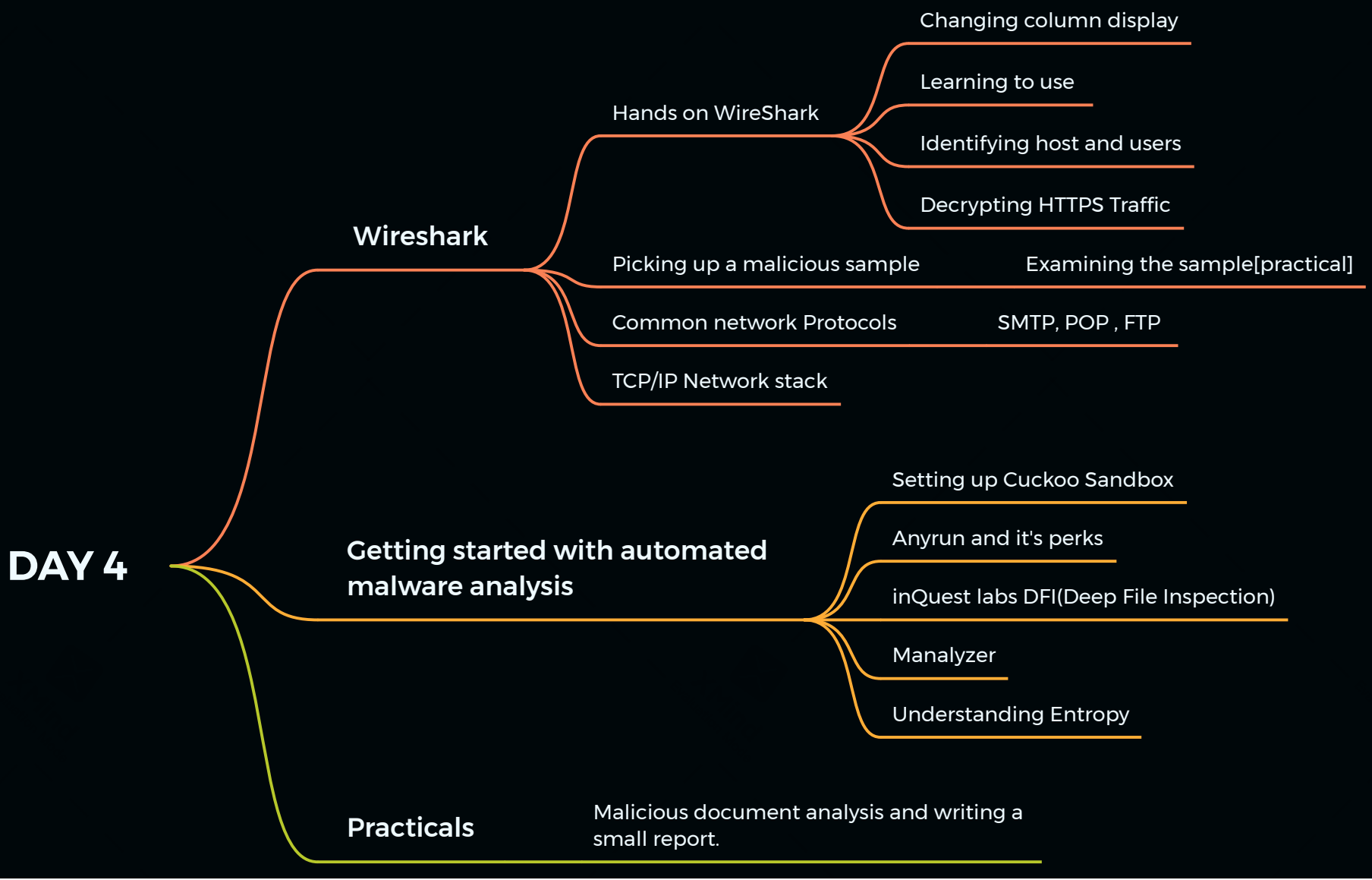
DAY 4
Wireshark
Hands on WireShark
Changing column display
Learning to use
Identifying host and users
Decrypting HTTPS Traffic
Picking up a malicious sample
Examining the sample[practical]
Common network Protocols
SMTP, POP , FTP
TCP/IP Network stack
Getting started with automated malware analysis
Setting up Cuckoo Sandbox
Anyrun and it's perks
inQuest labs DFI(Deep File Inspection)
Manalyzer
Understanding Entropy
Practicals
Malicious document analysis and writing a small report.