- stack memory
- ida pro
- cyber warfare any case study expain dil and any dll with function service
- define assembly language
- rootkit
- plain text and cipher text
- debugging with staging
- malware and malware family
- pe header
- describe kernal mode and how kernal debug work goal of malware Analysis 8 marks
- static linking, run time linking and dynamic linking
- volatile data expalin digtal forensics
- elobrate malware process injection
- c code in assembly language
- expalin six level of
- what is memory forensics and step to perform
  memory forensix
- binding malware and obfuscation of malware
- paper 2
- threat intelligence
- yara signature
- debugger with functions
- encoding encryption hash
- define sandbox
- assembly debugger
- decribe user debugger mode
- malware family
- difference between dissembler and debugger
- explain analysis of obfuscated hostile code
- describe pe file and analysis
- what is static analysis
- explain case study of malware Analysis of malware forensics
- type of breakpoint
- define step of malware Analysis lab step
- what is registry and types off register
- dynamic analysis and step of dynamic analysis malware Analysis requirements