

CSCN4021 Cyber Crime Investigations

Examination & Analysis of evidences

Course Co-Ordinator

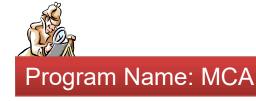
Dr. Jayakumar Assistant Professor Department of Computer Science and Engineering Galgotias University





Examination

- Higher level look at the file system representation of the data on the media
- O Verify integrity of image
- MD5, SHA1 etc.
- Recover deleted files & folders
- Determine keyword list
- What are you searching for
- Determine time lines
- What is the timezone setting of the suspect system
- What time frame is of importance
- Graphical representation is very useful





Examination

- Examine directory tree
- What looks out of place
- Stego tools installed
- Evidence Scrubbers
- Perform keyword searches
- Indexed
- Slack & unallocated space

- Search for relevant evidence types
- Hash sets can be useful
- Graphics
- Spreadsheets
- Hacking tools
- Etc.
- Look for the obvious first
- When is enough enough??

