# Cyber Security-Edge Program

|  |
| --- |
| Name: Afrin Faria  ID: 2111270  Batch: B11 |

|  |
| --- |
| 4. 21 September 2024  OSTIN : open source  <https://www.virustotal.com/gui/home/upload>  Link theke report  <https://poe.com/login>  <https://claude.ai/>  <https://app.any.run/>  <https://leakpeek.com/>  Download ch9 from “**https://drive.google.com/drive/folders/1Hml0pNjWsS0JUX2\_mXRxXPtcNjP0fz69**”  Create a folder in windows  Select shared folder in oracle , create new , add a path of a folder,  Click auto mount and permanent  **Getting a picture from a disk analysis their location:**  In kali :  Sudo -i  Cd /media/sf\_cyber  [cd /medis/sf\_folderName]  Ls  Ostin: Find the cat location from the disk file  Apt install testdisk  #to test the file  Testdisk ch9  # press enter INTEL —> advanced : filesystem units → fat32 → list →    Files → revendications.odt → PRESS C twice →  # In windows check shared file  # change the file location to .zip  View →show → file name extension → change to .zip  #extract all  #go to kali  Apt install exiftool  Cd /media/sf\_cyber/Files/revendictions/Pictures  Exiftool picture\_name.jpg  GPS Latitude : 47.6  GPS Longitude: 7.4  <https://www.gps-coordinates.net/gps-coordinates-converter>  Get address  <https://osintframework.com/>  Report on threat intelligence any 3 topics.  #osintleak.com username and password diye  ?intitle:index of? movie 3 idiots  DorkGpt  exploit-db.com  Assignment: <https://www.exploit-db.com/google-hacking-database>  wappalyzer.com – to check stacks  How to get access to the free CCTV .  <https://polyswarm.io/>  <https://www.hybrid-analysis.com/>  https://urlscan.io/result/8205e9fe-fae2-4465-ac88-31e05e9905df/  Domain information: https://talosintelligence.com/  Poralekha 6ta category <https://abuse.ch/>  IOC  <https://tryhackme.com/r/room/threatinteltools> |