SONU MANDECHA

☎ +91 8178410303

✉ drsonamandecha@gmail.com

in https://www.linkedin.com/in/sona-mandecha-28a6aa16a

Career Goals

I want to be a passionate Cyber Security and Cyber Forensic Expert I am curious and enthusiastic to know about the latest technology, to address new issues and learn new things.

Education

S. No.	Courses	College/School	University/Board	Year of passing	Percentage/CGPA
1.	M.Sc. (Forensic Science) with specialization in Cyber Forensic	LNJN-NICFS	Guru Gobind Singh Indraprastha university (GGSIPU)	2020	Sem1- 8.8 CGPA Sem2 -8.7 CGPA Sem3- 9.2 CGPA
2.	B.Sc. (Forensic Science)	Amity Institute of Forensic Science	Amity University	2018	7.4 CGPA
3.	Class 12	Modern Vidya Niketan	Central Board of Secondary Education (CBSE)	2014	90%
4.	Class 10	Holy Child Public School	Central Board of Secondary Education (CBSE)	2012	10 CGPA

Workshops

- One day workshop at Centre for Development and Advanced Computing Centre (C-DAC) (5 March, 2019).
- Two days' workshop at National Crime Records Bureau, Central Fingerprint Bureau (October 9, 2018- October 10, 2018).
- Two days' workshop in "Future of Forensic Science", Acharya Narendra Dev College, Delhi University, New Delhi**.**

Internship

S. No.	Institution	Duration	Year
1.	Information Sharing and Analysis Center	2 months	15 July 2020- 15 September 2020
2.	Cyber Prevention, Awareness and Detection Center (CyPAD)- Delhi Police	30 days	03 June 2019- 30 June 2019
3.	Rohini Forensic Science Laboratory	15 days	20 December 2018- 05 January 2019
4.	Indian Cyber Army (Cyber Crime Investigation)	15 days	23 July 2018-
5.	Hindu College, Ramjas College (Document examination)	15 days	01 July 2018- 15 July 2018
6.	Rohini Forensic Science Laboratory	30 days	17 June 2017- 17 July 2017

Technical Skills

▪ Information Security

▪ Good knowledge of TCP/IP protocol and Network Analysis.

▪ Strong technical knowledge of network technologies such as Firewalls, IDS/IPS solutions, VPN, LAN.

▪ Performing Forensic analysis for security incidents.

▪ Good knowledge of System Security Requirement

▪ Knowledge of OWASP TOP 10 vulnerabilities.

▪ Familiar with working knowledge of Operating system; Windows and Linux.

▪ Hands on Knowledge on Various Ethical Hacking, Network Scanning and Web Application Security scanning tools such as Nmap, Metasploit, Nikto, Burpsuite, Masscan, Arachini, Acunetix, Sqlmap, Metasploit.

▪ Hands on Knowledge on the operation of "Splunk" tool.

▪ Disk Forensics-

▪ Good technical expertise and experience in conducting Imaging of the suspected media. Tools used are- Acquire Data FTK Imager, SOLO4, Cyber Check Suite, Trueback and Media Clone.

▪ Good technical knowledge in recovering deleted files and folders and their analysis using Puran file recovery, Autopsy, FTK Analyzer, EnCase, Cyber Check Suite and Recuva file recovery

▪ Sound technical knowledge in Anti-forensic techniques like data hiding and recovery of the hidden data. Tools used are- Steghide, SNOW for Steganography and Aletheia tool for Steganalysis.

- Good knowledge in analyzing Windows Registry as well as recovering the deleted keys. Tools used are- Registry Explorer, FTK Registry Viewer**.**
- Good knowledge in analysis using Hex Editor.
- Good knowledge of FAT and NTFS file system.

- **Live Forensics**

- Good technical knowledge in collection and preservation of volatile data.
- Tools used are- Winlift Image builder, Winlift Imager, Winlift Analyzer, Magnet Ram Capture

- **Network forensics**

- Good technical knowledge in analysis of network traffic, analysis of Packet capture file (Pcap file).
- Good knowledge in scanning of networks to identify open ports.
- Tools used- Nmap, Wireshark, Masscan, Metasploit

- **OSINT**

- Good knowledge in different Tools and techniques used for information gathering on social media platforms.
- Tools used- community edition of Maltego.
- Tools used – Harvester, Sublister, Wappalyzer, Amass, Google Dorks, Shodan.

- **Mobile Forensics**

- Good knowledge in various acquisition techniques for mobile phones.
- A good hand on practice on -Oxygen Forensic kit, Cellebrite UFED 4PC, Cellebrite Reader, Mobile check suite 4.0 for acquiring and analyzing data from seized Mobile Devices.
- Call data record analysis using Advik CDR Analyzer.

- **Docker Analysis**

- Good knowledge in developing docker containers and installing forensic tools in the container.
- Good knowledge in analysing docker containers.

- **IOT**

- Good knowledge in firmware simulation and exploitation.

Training

- Five days Masters Level Training Course in Cyber Forensics from **Centre for Development of Advanced Computing, Noida.**

Projects

- Summer project on “Plastic Currency” in Amity University, Noida, UP
- Presentation on “Anti- Forensic techniques” at LNJN NICFS, Rohini, New Delhi.
- Final semester dissertation on the topic “**An Empirical Study of Digital Forensic Tools and Techniques for Detection of traces of Anti-Forensic activities in USB storage devices and Windows Artifacts**”

Publications

- Published a research paper on "**A Comparative Study of the Performance of Open-Source and Proprietary Disk Forensic Tools in Recovery of Anti-Forensically Doctored Data"** in **International Journal of Cyber Security and Digital Forensics** journal.

Work Experience

Currently working as a Cyber Security Analyst in International College for Security Studies (ICSS) from October 1, 2020.

Ongoing Certifications

- Currently pursuing **CEH (**Certified Ethical Hacker) and **CPT (**Certified Penetration Tester) from ISAC.

Certifications

- A certificate of achievement for "Information Security Incident Handling" from "Charles Sturt University".
- A certificate of completion of "Practical Ethical Hacking- The Complete Course" from "Udemy".
- A certificate of completion for "CNSS Certified Network Security Specialist" by "ICSI"
- A certificate of completion of "Introduction to Cyber Security" by "Cisco".
- A certificate of completion for Foretinet NSE-1 by "Fortinet".
- A certificate of completion for "Splunk 7.x Fundamentals Part 1" by "Splunk".
- A certificate of completion for "Splunk Infrastructure Overview" by "Splunk".
- A certificate of completion for "Splunk User Behavior Analytics" by "Splunk".
- A certificate of completion for "AccessData Certified Investigator" by "AccessData".
- A certificate of achievement for the completion of "Autopsy 8- Hour Online Training." By Basis Technology.
- A certificate of attendance for the completion of "Cellebrite Reader Course" by "Cellebrite".

Languages

- Hindi
- English