Saurabh Pathak
MS (Digital Forensics & Info. Assurance), GCFA, C|HFI
Contact No: +91-8511553664,
Email: talk.saurabh@hotmail.com

Objectives

To be a Technical expert in the field of information exchange technologies and Information Security Management systems by gaining practical experience and intellectual skills while working on operational position in a high growth organization of same field.

Technical Skills

- **Computer Forensics:**
  Evidence imaging, extraction of data using Forensics Tool Kit and various other open source tools. Analysis of volatile and non-volatile data on Windows operating systems. Recovery of deleted files and partition using different forensics techniques like file carving.
- **Incident Handling and Investigation:**
  Incident detection, analysis and reporting based on implemented guidelines and procedures. Perform triage, containment and Incident Neutralization activities. Basic Understanding of compliance standards, India IT act 2008.
- **Intrusion and Network Analysis:**
  Understanding of network and application protocols, understanding of packet headers and data, hands on experience with network capture and analysis tools like Wireshark, Fiddler analysis suite.
- **Malware analysis:**
  Perform static and behavior malware analysis of malicious Windows executables files under sandboxed environments. Perform memory analysis for advance adversaries.
- **Data Analytics:**
  Analyze logs collected from various sources. Generate charts, reports, diagram to identify patterns and determine best actions for assigned investigative task. Hands on Experience with tools like Carbon Black, McAfee ePO console, FireEye etc.
- **Timeline Analysis:**
  Timeline analysis is useful for a variety of investigation types and is often used to answer questions about when a computer is used or what events occurred before or after a given event.
  Tools used: Plaso, log2timeline, psort, mactime etc…
- **Other Skills:**
  Tools such as FTK, Carbon black, Sysinternal suit, Anomaly threat stream, FireEye for email security, Nirsoft suit, and various open source tools to perform various forensics investigations, incident response and malware analysis. Understanding of various network architecture. Hands on experience with various operating systems. Forensics reports writing to present respective authorities/legal team.

Professional Experience

1) **Fiserv Global services,**
   Information Security Analyst **Oct 2015**

- Member of Cyber Security Incident Response Team (CSIRT) which is a specialized group within Fiserv, for sole purpose of combating and responding to security incidents.
- Provide comprehensive computer forensic investigation: Acquire, collect, document and preserve evidence from various forms of electronic media and equipment.
- Find out the IOC (Indicator of Compromise) from the analyzed suspicious files and place the block

on endpoint and network levels.
- Respond immediately to security-related incidents and provide a thorough post-event analysis.
- Anticipate security alerts, incidents and disasters and reduce their likelihood.
- Conduct highly-confidential internal investigations related to violations of Acceptable Use Computing device Policies and other activities counter to the organization's success.
- Analyze malware, extract indicators and create signatures. Perform network scan for malware, Software package non-compliance on user systems and servers.
- Analysis and handling of malware in safe manner to avoid further spreading in network, which were came due to different methods into organization network and not having signature to different security controls to remove those. Submit the finding different business units.

2) SNR Pvt. Ltd.,
Technical Consultant **Jul 2012 – Aug 2013**
Responsibilities:

- Installation, Configuration of Server and networking on Centos 5.5.
- Handled the tasks of diagnosing and resolving technical problems in Linux (Centos5.5).
- Imaging and extraction of data using Forensics Tool Kit (Imager Lite), Encase and other data recovery technique in case of data lost.
- Training the manpower and coordinate with senior administrative officers.

Academic Profile

Name of School/college/ university attended	Qualification	Board Year	Percentage/ Grade
Gujarat Forensic Sciences University, Gandhinagar, Gujarat	MS-DFIA	2015	B
UPTU	B.Tech (EC)	2011	63%
S.G.M Indira Nagar, Kanpur	Intermediate(Math)	2006	71%
S.V.M Higher Secondary School, Kalpi	High School(Math)	2004	65%

Technical Certificates

- GAIC Certified Forensics Analyst (GCFA)
- Certified Hacking Forensic Investigator (CHFI)
- EC-council Certified Ethical Hacker (CEH)
- Certified System Security Analyst (CSSA)

Professional Project Experience

Title: "Virtual Training Environment" - Alok Tripathi Scientist (D)
Tools: VMware, Wireshark, IDS/IPS and various other security tools.
Description: To develop a virtual training environment for enhancing the IT Security skills among IT professionals and students.

Academic Projects Experience

Title: “To Study and Design H Shape Micro Strip antenna” - **Prof. Amit Gupta.**
Platform: Zealand IE3D
Description: To study and design a micro strip antenna which has advantage of low profile, low Cost, and ease of fabrication and finding the application in a wide range of Microwave Systems.

Cost, and ease of fabrication and finding the application in a wide range of Microwave Systems.

Area of Interest

- Information Security
- Digital Forensics
- Malware Analysis
- Risk Assessment & Management.
- Security Governance and Policy adviser.
- Communication Systems and Information Exchange Technologies.

Personal Skill

- Good problem solving ability and analytic skill to solve the problem efficiently.
- Good communication skill, creativity and capability to organize.
- Recognized for effective Team Player, skilled Trainer and Motivator.

Extra-Curricular Activities

- Leisure Interest: Photography
- Guitar.
- Social works.

Personal Details

Date of birth	**:** March 13th, 1991
Language Known	**:** English, Hindi
Nationality	**:** Indian
Gender	**:** Male
Strengths	**:** Optimist, Hard worker.

Declaration

Place: Signature
Date: (Saurabh Pathak)