Joseph Y Naghdi CV

Digital Forensics Analyst
Computer Forensics Lab, 133 Ballards Lane, London N3 1LJ
Email joseph@computerforensicslab.co.uk, Phone 0203934 1070

Expertise

I am responsible for investigating and analysing data extracted from digital devices and systems to uncover, preserve, and present digital evidence in support of legal, criminal, and corporate investigations. My role involves examining computer systems, networks, and mobile devices to identify and recover and analyse data that is crucial to investigations, while ensuring the integrity and chain of custody of the digital evidence.

I lead and coordinate computer forensic investigations, e-discoveries and perform advanced data recovery assisting clients within the legal profession and the police in gathering, organising, reporting, and presenting digital evidence in civil and criminal proceedings as well as offering computer expert witness services to defence lawyers, barristers and UK Crown Courts.

I specialise in gathering, capturing, analysing, examining electronically stored information, and reporting on it by making use of the most current and technologically advanced hardware/software tools. I have been assisting law firms, police forces, government agencies, local councils, fraud investigators, insurance companies, private individuals, and financial institutions with digital forensic investigations since 2007.

Experienced in digital forensic examinations in criminal prosecutions, civil litigation, PCI DSS forensic investigations and GDPR-compliant incident analysis and reporting. Key skills include forensic examination of computers, mobile devices, social media and cloud computing using a variety of forensic tools including EnCase, X-Ways, FTK, Nuix, Oxygen Forensic® Detective, Magnet Forensics, XRY and Cellebrite UFED. Joseph also specialises in E-discovery, EDRM with extensive knowledge of data collection, data carving using data processing tools such as Hex Editors, FTK Imager, CAINE, DEFT, Nuix and Relativity.

Core Skill and Competencies:

- **Evidence Collection:**
  - Identify and secure digital evidence from a variety of sources, including computers, mobile devices, networks, and cloud environments.
  - Ensure proper documentation and chain of custody procedures are followed.
- **Forensic Analysis:**
  - Perform detailed forensic analysis on digital media to recover and analyse data.
  - Utilise specialised forensic tools and techniques to examine data structures, file systems, and artifacts.
  - Extract and analyse information from logs, registry files, internet history, emails, and other digital evidence.
- **Reporting:**

- Prepare detailed technical reports documenting the findings, methodologies, and tools used during the investigation.
- Present evidence and findings in a clear and concise manner to stakeholders, including

Additional Key Skills:

- Skilled in using forensic tool suites (e.g., Cellebrite, XRY, Autopsy, MobilEdit, Avilla Forensics, Sleuthkit, FTK etc.)
- Skilled in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).
- Skilled in analysing volatile data (e.g. Live memory acquisition and analysis)
- Skilled in processing digital evidence, to include protecting and making legally sound copies of evidence.
- Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.
- Skilled in identifying obfuscation techniques.
- Skilled in interpreting results of debugger to ascertain tactics, techniques, and procedures.
- Skilled in deep analysis of captured malicious code (e.g., malware forensics).
- Skilled in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump, 010 Editor).
- Skilled in recovering data from iPhone and Android Phones using open source and commercial tools
- Skilled in recovering data from Nand flash, SSD and memory stick, memory card and chip-off methods using open source and commercial tools and hardware, NAND Adapters by Rusolut and Ace Lab PC3000
- Skilled in conducting bit-level analysis.
- Skilled in analysing memory dumps to extract information.
- Knowledge of reverse engineering concepts.
- Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro). (K0188)
- Knowledge of binary analysis.
- Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
- Knowledge of data carving tools and techniques (e.g., Foremost, Recovery Explorer, R-Studio, PC 3000).
- Knowledge of anti-forensics tactics, techniques, and procedures.
- Knowledge of concepts and practices of processing digital forensic data.

Work History:

March 2009 to Current: Computer Forensics Lab, London, Digital Forensics Investigator, Expert Witness in Several Criminal and Civil Cases in UK Crown Courts

Job role:

- Identifying, acquiring, capturing data sources, gathering digital evidence, analysing facts and trends and presenting the findings in format admissible in any litigation or reliable in a civil or criminal investigation.
- Was involved in detailed and comprehensive specific data search items such as emails, images, documents, spreadsheets, logs, chat conversations etc in all digital data sources such as hard drives, memory sticks, media players, mobile phones and network or remote drives.
- Implemented company policies, technical procedures, and standards for preserving the integrity and security of data, reports and access.

- Designed strategic plan for best practices in computer forensics investigations and data handling for training and supporting team members and outside contractors.
- Responsible for all digital forensic investigations and digital evidence acquisition from computers, mobile handsets, vehicles, CCTV and producing many expert reports based on the instructions given by the stake holders.

Typical Cases Supervised or Handled:

- Investigating computer and digital media involving data security regulatory compliance such as Data Protection Act and GDPR.
- Company information theft digital evidence gathering, reporting and auditing.
- Digital document authentication and validation in case where digital document or the evidence is disputed.
- Internet and online banking fraud investigations and reporting.
- Online bullying, stalking, trolling and defamation digital evidence gathering and reporting.
- Child pornography digital evidence gathering, examination and reporting for law enforcement, prosecution, and law firms.
- Acquiring and investigating digital evidence involving divorce cases
- Computer fraud investigations involving email impersonation, forging legal documents such as wills, contracts, title deeds, power of attorneys and bank statements.

August 2003 to Current: *Data Recovery Lab London, Data Recovery Specialist:* My role involves training, supervising engineers and leading the data recovery lab technicians. I recommend architectural improvements, design solutions and integration solutions for improving working practices in the lab.

May 1996 to June 1999: *BBC World Service, Bush House, London, Producer/Presenter:* My role was to produce news and current affairs programs in BBC World Service located in Bush House in London. I managed a team of 5-6 journalists, assistant producers involved in producing. editing and presenting news and current affairs with a primary focus on Iran and the Middle East. In February 1999, I was asked to join a consultation team commissioned to devise and suggest the best digital format to present the news in what later became BBC News Online.

Education:

1991 Tehran Technical College Tehran, Iran
MSc (Master of Science) in Computer Science + C Programming
1984, Ferdowsi University Mashhad, Iran
Bachelor of Science, History of Western Philosophy

Affiliations and Memberships:
IEEECS (Institute of Electrical and Electronics Engineers Computer Society), Member
BCS – The Chartered Institute for IT, Professional Member

Certifications:

Microsoft Certified Solution Developer (MCSP)
Certified Information System Security Professional (CISSP)
EnCase® Certified Examiner (EnCE)
Microsoft Certified Professional (MCP)