KROLL

Nick Ellison

Senior Director

Contact

E nick.ellison@kroll.com

T +44 (0)207 029 5498

M +44 (0)722 102 6619

Skills & Qualifications

- Holds an MEng in Systems Engineering from the University of Warwick
- PRINCE2® Practitioner
- Programming languages including Python, Ruby, C++, PHP, JavaScript
- Proficient with cloud infrastructure, AWS Certified Cloud Practitioner
- Database/analytic techniques including SQL (MSSQL. PostgreSQL, MySQL), Power BI
- Data science & machine learning experience using R and Python
- Proficient with EnCase®, Axiom, Intella, Relativity, Reveal-Brainspace, and a range of eDiscovery tools
- TRM Labs certified in Digital Forensics and Cryptocurrencies, and Advanced Crypto Investigator
- Member of the Chartered Institute for IT
- Member of the Society for Computers and Law
- Member of the Institute of Engineering Technology
- Associate Member of the Academy of Experts

Nick Ellison is a Senior Director in the Data Insights and Forensics practice, based in London. Nick has more than 15 years of IT technology consultancy and software development experience. He has assisted clients with web and software development projects, disputed and delayed delivery of projects, fitness for purpose assessments, IT security controls, digital forensics, and cyber risk in the travel, AI, crypto, manufacturing, wholesale and distribution, financial services, charities/third sector, and hospitality sectors. He specialises in technology disputes involving software intellectual property and fitness-for-purpose.

Prior to joining Kroll, Nick founded a software development consultancy and a web development agency for the professional services sector. He has also co-founded several startups in a CTO capacity and has given expert advice on a range of technology implementation projects for third parties. Prior to that, he was a consultant at Deloitte in the Data team of the Enterprise Risk Services division.

Representative engagements

- Instructed as an expert witness to opine on the suspected theft of Artificial Intelligence (AI) models from a Software-as-a-Service product by the previous management of a software company following an M&A transaction.
- Instructed as an expert witness, giving written testimony in court relating to whether an algorithmic trading company had properly disclosed source code compliant with a court order.
- Instructed as an expert witness to opine on the best practice of an outsourced software development team for a leading sports data aggregator. Nick's findings were presented in a CPR35 report, followed by a joint expert's report produced in coordination with the opposing side's expert.
- Instructed as an expert witness to opine on the extent to which an e-commerce platform had been successfully delivered by a supplier to the retailer, and whether bugs allegedly present in the work product would have constituted material defects.
- Instructed as an expert witness to opine on suspected source code theft in a Point-of-Sale application on an Android-powered payment terminal. Conducted black box comparison exercise, reverse-engineering of application executables, and reviewing for evidence of potential artefacts.

- Instructed as joint expert witness to opine on suspected manipulation of email metadata relating to financial transactions.
- Supported the investigation and supplemental expert delay report for a high-profile government department software implementation dispute.
- Assisted a leading global cryptocurrency exchange with reviewing geofencing protocols, testing IT controls of both website and mobile application touchpoints, reviewing operational data logs, and making advisory recommendations for areas of improvement. Nick presented the findings to the General Counsel of the firm and leadership team.
- Provided supporting technical analysis to an expert appraisal and valuation of a suite of hospitality technology tools in relation to a high-profile family dispute which was prompting the breaking up of a business empire.
- Assessed misuse of confidential information in an airline industry payment software arbitration matter, determining how a competitor product could have been reverse-engineered.
- Led the investigation into a UK Gambling Commission compliance issue for a gambling software company, reverse engineering user activity from server logs and reviewing source code to support findings.
- Investigated suspected intellectual property theft from air ticketing booking software integrating with a travel GDS service, through review of source code and data from a limited number of intermittent backups.
- Investigated suspected source code theft for medical device firmware, by reverse engineering software binaries and developing mass processing techniques to identify potentially matching strings in included libraries.
- Led forensic investigation of email metadata across multiple inboxes from three different parties for evidence of the source of a successful payment scam targeted at a film studio.
- Assisted the forensic investigation of email and document data for an investment firm where a member of senior management was suspected of having manipulated emails for personal gain.
- Conducted forensic email examination on a range of communications with purported investors relating to a major fraud investigation of a tech unicorn.
- Led the digital forensic investigation relating to a major IPO, where key individuals had been linked with historic cybercrime and scamming by investigative journalists. Nick led interviews with the client's staff and developed a detailed history of the

major players concerned, including previously undiscovered personal and business relationships. Additional concerns were identified and shared with the client.

- Developed automated processes to identify unlicensed intellectual property in hundreds of public websites and compiled mobile applications for a leading global retailer with multiple sub-brands. Nick identified $10m of exposure that the client was able to mitigate through a settlement deal.
- Investigated the suspected theft of pharmaceutical products from a warehouse that had been covered up through the manipulation of the in-house ERP system. Nick designed SQL analysis processes to perform additional reconciliations to identify disparities in data that had been initially covered up and presented these findings to the client.