Mr Thomas Moore **MBCS MEWI**

thomas@tkmtechnologies.com
Tel. +44 (0)7798 845 862
Suite C, City House, 96a High Road, Nottingham NG9 2LF (UK)

SUMMARY

I lead the delivery of digital forensics and e-discovery services across a wide range of criminal, civil and regulatory matters, as well as corporate investigations. My approach is client-focused, grounded in trust, strategic insight and clear, effective communication throughout each engagement.

With a particular focus on regulatory and compliance matters, internal corporate investigations and complex, high-value litigation, I work closely with clients and their legal teams to align technical, legal and evidential strategies.

To date, I have managed more than 220 digital forensic investigations across EMEA, APAC and the Americas. I have also developed tailored training programmes in digital forensics and worked with law firms to integrate efficient and defensible forensics and e-discovery processes into their client services.

Areas of specialist skill...

- Development and implementation of digital forensics and e-discovery strategies
- Alignment of investigative priorities with forensics best practice to ensure defensible outcomes
- Leadership and management of digital forensics, e-discovery and incident response teams
- Delivery of digital forensics support in complex and rapidly evolving investigations
- Standards-compliant evidence collection, preservation and handling
- Mobile device, computer and cloud digital forensics
- Expert witness services, including report writing and courtroom testimony
- Cross-jurisdictional investigations, particularly across EMEA and Asia-Pacific
- Experience of working within ISO/IEC 17025 accredited environments
- Development and delivery of digital forensics and e-discovery training programmes

Highlights...

- Managed more than 220 digital forensic investigations across 22 countries
- Professionally accredited Member of the British Computer Society (MBCS)
- Professionally accredited Member of the Expert Witness Institute (MEWI)
- Experience of providing written and oral expert evidence in civil and criminal proceedings
- Previously cleared to UK HM Government SC security clearance level

---

KEY SKILLS

Investigative Practice & Expert Witness:

- Extensive experience of developing, applying and assuring best-practice in the identification, collection, forensic preservation and analysis of digital evidence
- Experience of working to statutory and sector-specific regulatory compliance objectives

- Practical experience of addressing GDPR and other compliance issues arising from data breaches
- Experience of leading digital forensics investigations in environments accredited to ISO/IEC 17025
- Professional accreditation as an expert witness with recognition by the UK courts
- Experience of providing expert reports in accordance with CPR 35, CrPR 19.4, FPR 25, IBA Rules on the Taking of Evidence and a range of other reporting standards
- Experience of delivering oral testimony under cross-examination in civil and criminal proceedings
- Experience of providing expert evidence in international arbitration proceedings

Technical & Tooling:

- Magnet AXIOM Cyber (for computer, mobile device and cloud forensics)
- Cellebrite UFED and Physical Analyzer (including Inseyets) for mobile device, cloud and embedded computing forensics
- EnCase Forensic Edition and a range of other tools (e.g. for live systems acquisition and analysis)
- Design, administration and management of e-discovery projects, using RelativityOne, Reveal and Intella TEAM / CONNECT (including the use of advanced analytics)
- Application of novel techniques to accomplish defensible PII review at scale (including the use of machine learning and AI-based natural language processing and named entity recognition)
- Design and use of intelligence mapping environments, using i2 Analyst's Notebook / iBase
- Use of SIEM technologies (e.g. Microsoft Azure Sentinel, Splunk) and endpoint protection systems (e.g. Microsoft Defender, CrowdStrike)

Expert Witness & Practice Training:

Training in the following areas has been provided through the Expert Witness Institute (EWI) and forms part of a programme of continuing professional development in accordance with EWI accreditation requirements.

- Excellence in Report Writing
- Courtroom Skills
- Civil Law and Procedure (including the Civil Procedure Rules, Part 35)
- Criminal Law and Procedure (including the Criminal Procedure Rules, Part 19)
- Periodic briefings, seminars and so forth covering new developments and practice changes

---

CERTIFICATES AND MEMBERSHIPS

- Previously cleared to UK HM Government SC security clearance level
- Professionally accredited Member of the British Computer Society (MBCS)
- Professionally accredited Member of the Expert Witness Institute (MEWI)

NOTABLE ROLES AND CASES

Digital forensics expert in a multi-jurisdictional insider threat investigation

In this case, a European cryptocurrency trading platform was alerted to a potential data breach by several private clients, who reported unauthorised use of their security credentials for the purposes of executing unfavourable trades. Suspecting an insider threat or supply chain breach, the client and their legal counsel appointed me to lead a digital forensics investigation. During the course of the engagement, my team forensically captured and analysed more than 30TB of data from a range of devices and cloud services across

several countries, coordinated interviews with complainants and staff members, informed crisis communications and assisted legal counsel in Europe and the United States in anticipation of litigation and regulatory action. The source of the breach was ultimately traced to a vulnerability in a key software application, which had been exploited by a disgruntled employee to exfiltrate sensitive client data.

Digital forensics and e-discovery lead in a financial services compliance investigation

In this high-profile case, a major investment bank was required to cooperate with a books and records compliance investigation, conducted by the United States Securities and Exchange Commission (SEC). Under instruction from legal counsel acting for the bank, I designed a data collection and security protocol, and coordinated the on-site forensic acquisition of instant messaging communications from the personal devices of more than thirty custodians. I oversaw the subsequent processing and multi-stage review of more than 14million communications by legal counsel for both the individual custodians and the bank.

Digital forensics expert in an ICSID arbitration

In this case, which was administered by the International Centre for Settlement of Investment Disputes (ICSID), I undertook a detailed analysis of communications evidence, which was derived from a proprietary instant messaging application and had been submitted by the nation state Respondent as alleged proof of the Claimant's links to a designated terrorist organisation. I produced a comprehensive expert's report, in which I identified several significant issues affecting the reliability of the messaging data.

Lead forensics investigator in a Swiss corporate insider threat investigation

This investigation was prompted by intelligence, which showed that the senior managers of a Geneva-based oil field developer were using the company's high-value software licenses to support and build the operating capacity of an unauthorised competitor business. I led the investigation, which involved a rapid deployment to Switzerland, and the recovery and analysis of several million documents, e-mails and audit records. The entire investigation was conducted in accordance with strict Swiss data protection regulations, which required careful consideration of data sovereignty issues and substantial on-site operations.

Digital forensics expert in HM Revenue & Customs v CD (a private limited company)

I acted under instruction from the defence in this case, which concerned an allegation by HMRC that CD had been complicit in a missing trader intra-community fraud (MTIC, or so-called *VAT carousel fraud*). It was alleged that the bank accounts of several ostensibly independent companies had been accessed from a common IP address, thereby indicating that all of the companies were under common control. I provided expert analysis in relation to the IP address evidence, along with a CrPR Rule 19.4 report, in which I noted that the IP address in question was not that of an end-user's internet connection, but rather a component of a large internet service provider's technical infrastructure and that it could not, therefore, be attributed to any specific party.

Digital forensics expert in R v JR

This unusually complex criminal matter centred around an allegation that JR, after leaving the employment of an IT service provider, accessed the computer systems of one of his former employee's clients and deleted various virtual servers, thereby causing widespread disruption, with losses and costs assessed at GBP£870,000. I produced a series of expert reports and joint statements (to CrPR Rule 19.4) and provided support to Counsel during the trial. JR was subsequently acquitted.

e-Discovery consultant in a high-value merger case

In this substantial merger case, I managed the e-discovery function, from evidence collection through to processing, culling, review and production. I advised on e-discovery strategy and workflow at each stage. I also drafted the organisation's standard operating procedure for the ingestion of Concordance load files into Nuix, in accordance with the requirements of their ISO 17025 accreditation.

Digital forensics consultant in an investigation into an alleged state coup

In this high-profile case, tens of thousands of users of a mobile phone-based instant messaging application were alleged to have been complicit in organising a state coup. I led a review of the technical and forensic reports produced by the state's intelligence agency and advised on the interpretation of evidence seized from a variety of sources.

Forensic examiner in a case involving modified software source code

In this rather unusual case, it was alleged that software source code had been modified to expose a vulnerability, which could be exploited by a member of the development team. Working with the developer, I led the analysis of the affected source code and examined the software's deployment lifecycle and commercial uptake to quantify the potentially affected systems and users.

e-Discovery consultant in a suspected information security breach

I led the digital forensics and e-discovery function of an investigation into suspected theft of data from a London-based hedge fund. I oversaw the identification and preservation of data and managed the provision of e-discovery services to a team of reviewers.

Digital forensics consultant in a sensitive document leak enquiry

I co-led the investigation, capture (overseas) and analysis of electronic evidence on behalf of an international consultancy group, who were tasked by HM Government with investigating a leak of sensitive documents from a location in West Africa.

Digital forensics consultant to a Competition Regulator

I supplemented the internal digital forensics investigation capability of the UK competition regulator. My role involved the management, coordination and examination of digital evidence in cases related to market manipulation and cartel activity. During this appointment, I reconstructed a large volume of complex and fragmented output from a previous e-discovery review such that material identified as relevant could be used reliably in formal legal proceedings.

Digital forensics consultant to a National Airline in the Gulf Region

I assisted a major flag carrier in investigating incidents of intellectual property theft, commercial espionage and anti-competitive behaviour. This was a particularly sensitive role since the reputation of the airline amongst its investors and employees was dependent on the management of the investigation. The outcome was a significant and continuing reduction in commercial losses attributable to IP theft and espionage.

Digital forensics investigator to a Financial Regulator

I provided a digital forensics investigation capability to a large financial regulator. My role was in relation to cases of financial crime involving issues such as cross-border market manipulation and insider trading. During this time, I coordinated the production of evidence for investigative review and developed new cloud-based applications to enable workgroup review of forensically recovered digital call recordings.

Digital forensics course instructor to a Middle Eastern Government Agency

I developed and delivered a series of training courses covering digital forensics and live analysis to the security services of a major Middle Eastern Government. This training was delivered using simultaneous translation into Arabic and involved a combination of lectures and live simulation exercises.

Flowtex Technologie GmbH (Germany) – Insolvency Proceedings

In this case – of one the largest corporate failures in German history – I recovered electronic records which indicated the location of a valuable asset required in insolvency proceedings, I traced the asset to Australia and obtained positive verification of its nature and precise whereabouts. I worked closely with the UK legal team and continually communicated my findings. This investigation was conducted under severe time constraints and successfully resulted in the secure recovery of the high-value asset.

REFERENCES

Due to the sensitive nature of my work, referees have requested that their details be provided only on request.