Alistair Ewing Bsc (Hons) ACE AME CCE CFIP COSFE CMFS EnCE XRY

Address 15 Old Bailey, London, EC4M 7EF
Telephone (0203) 5989658
Mobile 078280 04750
Email a.ewing@compute-forensics.com

Professional Profile

A dedicated and self-motivated digital forensic investigator with extensive experience creating innovative and effective investigation solutions for key clients such as Irwin Mitchell, Bark and Co, LDM Global, Tiffany's Jewellery and Domvs London. Able to effectively manage the end to end processes of investigation projects from original concept, through to development, production, and completion. Possesses excellent communication skills with the ability to build and develop mutually beneficial relationships with co- workers and key custodians while ensuring the adherence to ACPO guidelines. Extensive experience of all necessary investigation packages from Encase to FTK and Nuix. Works well as an individual or within a team demonstrating vital team leading skills and the capacity to motivate and empower staff into fulfilling their full potential while contributing to the electronic discovery forensic process and exceeding client objectives.

Daily experience with using industry standard tools i.e. EnCase, OS Forensics, FTK, FTK Imager, Solo, Tableau, Live Boot CDs, IEF, Password Cracking tools and NUIX. Knowledge of Windows, UNIX, Linux based OS and file systems, server topology and a range of server backup software/hardware awareness including extraction and cataloguing. A decent familiarity with cloud infrastructure and smart devices. Experience using mobile forensics UFED, XRY, OFS, MPE and USIM Detective.

Objective

Currently looking for challenging investigations/collection opportunities. I can provide an array of professional services and act within the ACPO guidelines.

Notable Cases

THE QUEEN -v- ASIL NADIR – Fraud

Nadir's trial commenced at the Old Bailey on 3 September 2010, on 13 specimen charges of false accounting and theft totalling £34m. He was found guilty of 10 counts of theft totalling £29m and on 23 August 2012 was sentenced to 10 years in prison. A document was discovered by myself that displayed that Nadir forged a letter which purported to be confirmation from a bank that the necessary funds would be remitted. This was done by looking at the metadata as well as clock changes on the system around that time using log2timeline. Due to the mitigating circumstances his sentence was reduced by 2 years and instead of having to pay compensation in excess of £ 60 million he was ordered to pay just £5 million. https://en.wikipedia.org/wiki/Asil_Nadir

R v SAINI – Insider Dealing

At the time the largest FSA prosecution into insider dealing relating to spread betting on derivative trades concerning share price movements. Bark & Co acted for the Defendant who was the link between the "inside source" and the trading Defendants. The evidence included statements from bankers within two large well-known banks, digital experts (including myself), experts in Price-Sensitive Information and Publicly Available Information. I worked on this as defence case instructed by law firm Bark and Co. I found that the prosecution stated that the price sensitive information in his Hotmail was 'saved' to his desktop, in fact it was only opened. The prosecution were wrong to say for definite the emailed

attachments were 'Saved' when they were cached. I did however, recover the communications that detailed price sensitive information and was able to rebuild the webpages as the user would view those using NetAnalysis. The report was a great help to legal counsel.
https://www.youtube.com/watch?v=9BaIEMX9paU

ST Bart's Hospital London – Data Recovery

I was instructed by Head of St Bart's hospital nuclear medicine department, Dr Neil G Hartman to recover a lost Firebird based database from the nuclear medicine database. Veenstranet, the company that designs the databases for medical use said that they weren't backed up properly so recovery was impossible. Using an empty database, was able to come up with custom carving query using custom carver suite to copy the header and footer for carving and FTK to carve from the forensic image using the custom option. The full nuclear medicine database was recovered from the image of the disk as the backups were produced incorrectly by copying a live SQL database.

Generali Insurance Company – Onsite Search of Servers

A dispute was filed against insurance company Generali. I had to find a complete document with little disruption to the live server. Using FTK v6.1 I attached a powerful server to the domain and entered it through a live agent that comes with FTK enterprise. The 10TB of data was parsed, searched with the results exported as an AD1 logical forensic image. This lead to the conclusion that the letter and subsequent emails were valid and not forged in any way.

Tiffany International Jewellers – Employee Misuse of Computer

Instruction by Shirin Aboujawde of Tiffany's the jewellers was received. The problem that needed investigation related to an HR manager deleted a number of relevant documents relating to 'Adoption Leave' possible changing them. Using FTK and log2timeline I was able to pinpoint the steps taken that showed that the culprit did indeed deleted and modify documents on the server using a particular terminal machine. The evidence was used against her at the tribunal.

R v Chau – Immigration

Mr Chau has his immigration under review by UK immigration control. Instructed by acclaimed barrister Celia Record the concern was that for freedom blogger Chau it wasn't safe for him to go back to native Vietnam. By examining his computer, blog and by trying to view his blog using a Vietnamese proxy IP address. I was able to ascertain that Chau's blog attracted a considerable following and was indeed blocked by the Vietnamese authorities. I produced a report persuading the UK authorities that it wasn't safe for Chau to go back to Vietnam.

LDM Global – 30+ EDiscovery Projects

I was responsible for over 30+ collections and onsite processing of EDiscovery projects. During this time I acquired knowledge on how to collect from a plethora of different sources while dealing efficiently with on the job challenges as they arose. Using Linux boot CD's, writeblockers and cloud-based collection tools I was able to collect from 1000's of different devices while efficiently meeting time and compliance objectives.

Merton Council – Rogue Employee

A dispute at Merton council lead to an instruction that required me to analyse an employee's laptop while they were still onsite. I had to push an enterprise agent unknowingly to the culprit and image/analyse the system remotely. It was found this rogue executive was trading during work hours and even had a private Virgin media internet access installed in the office as to evade the work network.

R v Ajrizaj – Kidnapping

Benjamin Waidhofer barrister at 9-12 Bell Yard provided me with an iPhone for analysis his client had been accused of kidnapping. Using root and dd image the device over WIFI and extract deleted image metadata and prove his client's innocence by tracing the coordinates and producing an A3 map of the pictures plotted against the times. The forensic search yielded more artefacts than the prosecution due to knowledge of the iOS filesystem, the acquisition of a historical backup over the cloud and the illustration of the plots on a large A2 map that influenced the jury and judge into acquittal.

Skill Set

- Case Management
- Computer Investigations
- Data Management
- Email Analysis
- Apple Mac Certified
- Forensic Imaging
- FTK, Encase & OS Forensics
- Expert Witness Testimony
- Incident Response & Supertimeline Production
- Internet Forensics
- Mobile Phone Forensics
- Collection from Blue Chip Firms

Career Summary

June 2012-Current LDM Global

Associate Global Data Collection and Professional Services Technician

> Responsible for the planning and executing global collections.
> Face to face dealings and conference calls daily relating to pending collections.
> Liaising with IT departments throughout the world to fulfil duties.
> Maintaining the firm's evidence handling requirements.

Key Achievements

> Able to bring new encryption, handling and collection procedures to the table in order to perform more efficient and cost effective collections in the future. Examples include a standardised exhibit sheet, online live collection report to stop constant emails on progress from clients, more efficient imaging use boot disks and use of ddrescue for on the fly data recovery of old faulty disks.

May 2012-Current Compute Forensics

Digital Forensic Expert Witness and Business Owner

> Responsible for the design and layout of computer forensic lab.
> Overseeing the entire life cycle of computer investigation projects, from the initial stages of concept of an investigation to analysis, reporting and the testimony client consulting stage.
> Attending and liaising with clients at meetings to effectively cater for their individual investigative requirements.
> Creating promotional campaigns in order to gain clients.
> Maintaining and developing the company`s POS library

Key Achievements

> Being the initiator of a new business building it using own skill and initiative right from the website design, to the accounting right through to actually performing the service myself.

2009-2012 X-act Forensics UK

Digital Analyst

> Performing similar duties as the above in a fully-fledged forensic lab learning key skills.

2003-2009 Mencap UK

General IT support

> Responsible for overseeing all aspects of IT support in a business focusing on building and developing beneficial relationships to retain and increase the client base.
> Accountable for computer networking the running of company services as well as handling all administrative duties including security issues.

Education and Qualifications

Apprenticeship: X-act Forensics
Degree: Human Biology/IT 2:1
Certifications: ACE Access Data Certified Examiner
AME Access Data Mobile Examiner CCE
Certified Computer Examiner
CFIP Certified Forensic Investigation Practitioner
COSFE Certified OS Forensics Examiner CMFS
Certified Mac Forensic Specialist EnCE Encase
Certified Examiner
XRY Mobile Phone Forensic Examiner

Key I.T. Skills

Proficient in the use of Encase, FTK, OSforensics, FTK imager, PRTK, Registry Ripper, IEF, Nuix and Caine.

Personal Details

Languages: English (Fluent) German (Basic).
Other: Motorbike Licence, Clear CRB.
Interests include: Motor biking, Weight training, Travelling, Gym, Stock Markets, Forex

2
BEDFORD ROW

To whom it may concern,

I was Counsel for a defendant charged with a VAT fraud at Canterbury Crown Court earlier this year. The alleged loss was in the region of £7,000,000. We had cause to instruct an expert to deal with issues relating to the client's computer and, in particular, lists of tens of thousands of entries of fraudulent invoice details that he had compiled. We instructed Alistair as he had previously worked with my instructing solicitors, Bark & Co.

The analysis we required was both complex and time consuming. Further, due to delays in releasing the computer hard drive to us, the report had to be prepared quickly. Alistair produced a very detailed report which addressed the issues extremely well within a couple of weeks of receiving the necessary data. All involved on the defence team, solicitors and barristers alike, were extremely impressed by the way the report was written. In particular, we were greatly assisted by the way Alistair managed to translate fairly complicated technical matters into plain, easily understood English.

I had cause to correspond with Alistair after the report had been prepared to obtain clarification of a few points. He was able to give me some of the information I needed immediately over the telephone. What he could not tell me there and then he provided in an email later on that day. I found the way he dealt with my queries to be very helpful and user-friendly, especially the speed at which he responded as there was not much time to lose before the trial.

In short, I would recommend Alistair to others seeking expert advice in any kind of case and would be happy to use him, and X-act Forensics, again. He did an excellent job for us and I am certain that he will continue to do the same for his other clients.

If you require any further information, please do not hesitate to contact me.

Yours Faithfully

Sandesh Singh

2 BEDFORD ROW LONDON WC1R 4BU
Tel: 020 7440 8888 • Fax: 020 7242 1738 • LDE 17
Email: [initialsurname]@2bedfordrow.co.uk • www.2bedfordrow.co.uk

RODNEY WARREN & CO

solicitors

Berkeley House
26 Gildredge Road
Eastbourne
BN21 4RW
01323 430430

To whom it may concern

I instructed Alistair Ewing on an Indecent Images of Children Case in August 2010. I was extremely impressed with the way he carried out the forensic report in accordance with my instructions in that the report was prepared in a user friendly manner.

Alistair kept me constantly updated with the progress of the report to ensure it was completed within the set deadline.

On the day of the Court Hearing Alistair ensured that he was contactable by phone to answer any queries that we had with the report and he was very helpful in assisting with any extra information we needed.

Overall I would not hesitate to recommend Alistair as an expert in this field.

Yours faithfully

Yolanda Pons
Rodney Warren & Co

O'garra's
solicitors

Our ref AN TT

Your ref

23 February 2012

To Whom It May Concern

I am employed by O'Garra's solicitors who specialise in serious fraud cases. In 2011 I instructed Alistair Ewing of X-Act Forensics to interrogate a hard drive and prepare a report thereafter. I instructed Alistair as he came highly recommended by one of my work colleague's.

The case he was instructed on was very complex as it involved a very sophisticated type of fraud. Alistair dealt with all of my queries in an efficient and prompt manner. He was able to provide me with a quotation at short notice and quoted my firm a reasonable amount for preparing an Expert Report. Alistair prepared a very detailed Report in a short space of time. I found Alistair's Reports helpful, concise and easy to understand.

A number of issues pertaining to our case arose some time after the report was prepared which required Alistair's further expertise. Despite the fact that Alistair was abroad on holiday at the time he took time out to speak to me at length in relation to my case.

I would highly recommend Alistair to anyone seeking advice on computer related matters and furthermore I would not hesitate to instruct him again. I trust this information is useful and should you have any queries, please do not hesitate to contact me.

Yours faithfully

O'Garra

Anjum Nazir
O'GARRA'S