



Profile

EVIDENCE TALKS

Trust us
www.evidencetalks.com

Executive Summary	4
Capabilities and Expertise	6
Training	10
Key Staff Biographies	11
Specialist Forensic Products	12

OUR GOAL

OUR goal at Evidence Talks is to establish strategic relationships with all our clients, resulting in a better understanding of your business objectives. This enables Evidence Talks to deliver services that are closely defined to meet your specific needs.

We feel the opportunities identified by our clients and the services offered by Evidence Talks are a complementary fit. We hope the information contained within this document will contribute to a valued and continuing relationship between our companies.

Since 1993, Evidence Talks has been helping organisations respond to the need for forensic preservation of digital evidence, analysis and production of key information. Our enviable experience and reputation in corporate, commercial and criminal investigations means our clients benefit from an efficient, cost effective, reliable, impartial and thorough service.

From digital forensic consultancy and services to INFOSEC policy reviews, forensic training to forensic process integration, internet investigations to mobile phone forensics, we can provide one of the most comprehensive solutions available.

We are also proud of our software and product development capabilities which have produced some of the most innovative forensic solutions on the market for performing email forensic investigations, remote forensics and more.

As ‘expert witnesses’ we are called upon to present often complex technical evidence in a way that can be clearly understood by non-technical audiences. You can also benefit from this skill when we explain your options and the results of an investigation in clear, easy-to-understand language.

Our philosophy is simple:

- Work with you to provide the best level of service and technical competence
- Provide you with the right support, whenever and wherever you need it
- Keep the fee scales realistic

We look forward to working with you, when you need us, and to providing you with a professional, discreet, economic and reliable service.

History

Evidence Talks Limited is one of the longest established digital forensics consultancies in the UK, having started life as 4Warn Limited in 1993.

We have since been involved in a wide and diverse range of forensic examinations. The company is a member of F3, the leading forum for forensic practitioners in the UK.

Our founder and principal consultant, Andrew Sheldon — who has an MSc in



Forensic Computing — has a background in desktop audit, software licence compliance and abuse investigations. He has conducted thousands of forensic examinations and is a member of the Centre for Forensic Computing at the Royal Military College of Science at Cranfield University.

Andrew is also a member of the management committee for the MSc degree in Forensic Computing offered by the university as well as being one of the degree module designers and lecturers.

He is a regular speaker at national and international conferences including the NHTCU sponsored e-Crime Congress and Tackling Organised Crime conferences.

Specialist Facilities

We operate internationally from our purpose-built, secure and fully equipped forensic facilities based in Milton Keynes. We are within easy reach of all major cities in the UK and mainland Europe.

To provide a quick service to our international clients in the USA, Europe and beyond, we have formed strategic relationships with a select number of world-leading partners who can offer digital forensic, investigation and INFOSEC services to the exacting standards we require.

These partners have proved themselves to be among the best in their business and we are proud to be associated with them.

By working so closely with our partners, we can offer you a seamless continuity to all projects with a consistent management approach and unparalleled quality of service.

Specialist Development

Within our experienced team of professionals, we have a number of in-house developers who can respond quickly to demands for specialist tools to enhance our highly skilled forensic team and their current toolsets.

OUR SKILLS AND STRENGTHS

ALL our staff are fully trained and experienced in the use of numerous forensic tools and utilities, and work to the latest standards for digital evidence handling, reporting and forensic analysis. Whether the casework we undertake for you is criminal or civil, we have the skills, training and practical experience to provide a comprehensive service.

Forensic Incident Response

We can provide rapid response on site (covert or overt) as well as lab-based forensic imaging of digital media including PCs, servers, networks and removable media. We use a number of industry-standard methodologies and forensic applications including Encase FTK, Safeback and Linux DD.

Forensic Investigations

We conduct forensic examination and analysis of a wide range of digital media including hard disks, floppy disks, CD and DVD media, mobile phones, organisers (PDAs), digital storage cards (such as SmartDrive, CompactFlash and memory sticks) printers, fax machines, SANs, NASs, email systems and so on.

In fact, we pride ourselves on conducting leading edge research and developing forensic protocols for the examination of some of the more exotic forensic and

unusual devices, such as satellite navigation systems, games consoles and television access control systems.

Internet Investigations

Working with our strategic partner, ICG Inc, we provide a comprehensive range of covert internet investigation and analysis including email analysis, packet capture, web profiling, identity determination, posting and visibility monitoring, domain control mapping, identification of malicious posting sources, intellectual property intelligence services and internet risk/threat mitigation.

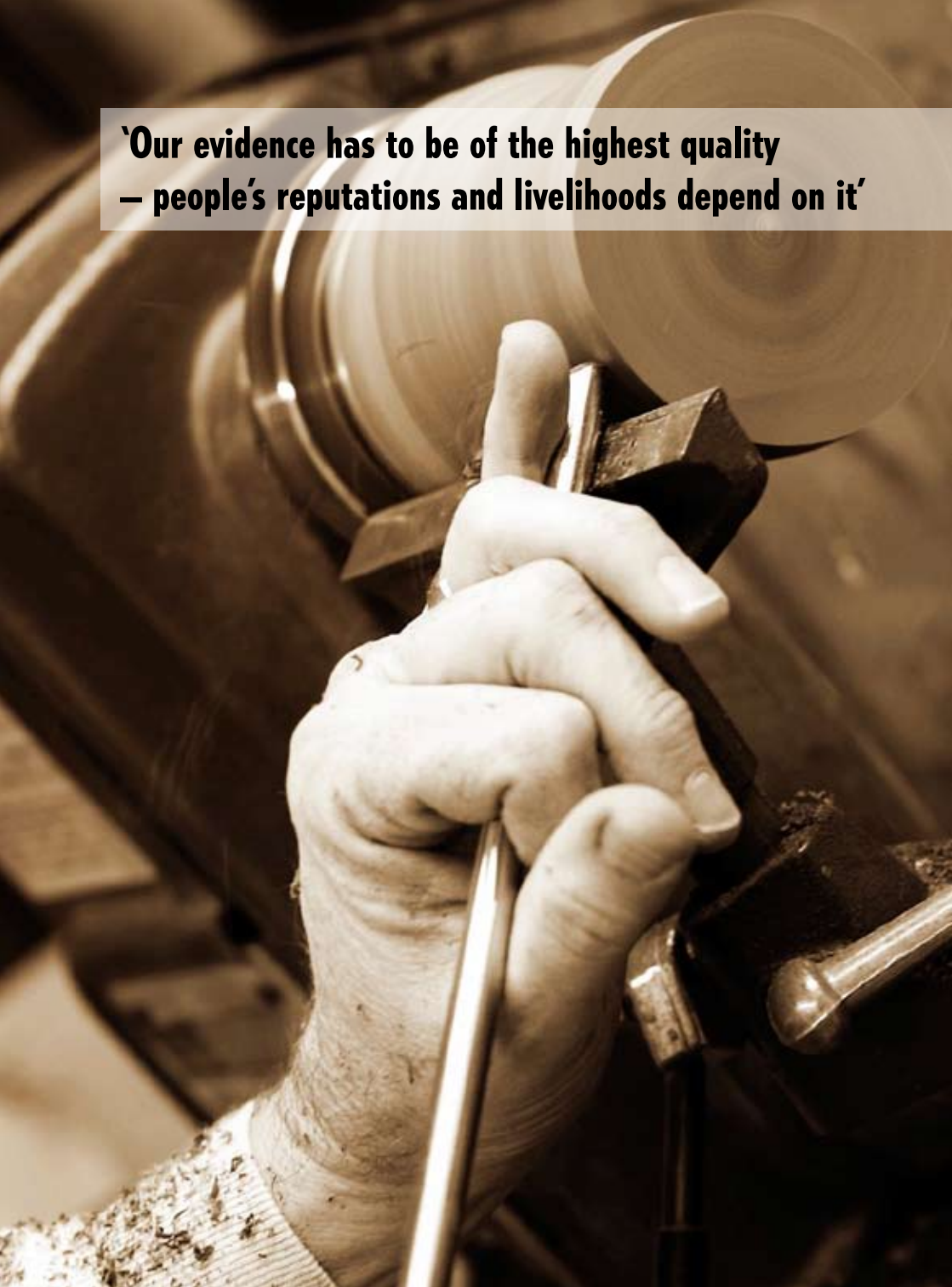
Using highly-specialised proprietary software and hardware, coupled with our sophisticated human intelligence operations, we have the capability to mine information from the parts of the net that are not normally open to public scrutiny.

We can correlate vast volumes of disparate intelligence into meaningful information, giving us the ability to investigate threats to your products, intellectual property, market channels and reputation.

Information Security Assessments

We conduct information security, IT security and physical security policy and procedure audits using trained and accredited staff.

**'Our evidence has to be of the highest quality
– people's reputations and livelihoods depend on it'**



Information Security Evaluations

External and internal penetration testing using NSA-approved technical consultants and methodologies.

(Typical Assignments)

- Network Vulnerability Assessment
- Attack and Penetration Testing
- Security Vulnerability Resolution Support
- Security Architecture Review and Development
- Security Policy Development and Implementation
- Intrusion Detection System Analysis and Implementation
- Firewall Analysis and Implementation
- Virtual Private Networking (VPN) Analysis and Implementation

eDisclosure and eDiscovery Consultancy

Services assisting either applicants and/or respondents to meet their objectives efficiently and economically.

Data Recovery Services

In the event of either logical or physical damage, we have the capability to recover data from all types of digital media including all RAID configurations.

Particular Expertise

Over the years, Evidence Talks Limited has built up considerable expertise in:

- Internet-related investigation into email abuse — in particular in tracing the source of malicious emails — software, music and video piracy/counterfeiting, brand damage, grey market and product diversion
- Theft and misuse of intellectual property
- Proving access to inappropriate content including pornography. Significant involvement in the investigation of child pornography distribution
- Abuse of corporate systems such as fraud and stock manipulation
- Data recovery in the event of malicious acts or accidental loss
- Password recovery and recovery of encrypted material following malicious acts or accidental loss
- Network forensics involving unauthorised access and abuse of access rights

OUR STRATEGIC PARTNERS

WE believe the best way of offering you the best services to meet all eventualities is to work with a small number of strategic partners who have been proven to deliver the best services in their fields at the most advantageous prices.

We are very pleased to count the following teams as long-term strategic partners.

Security Horizon

Specialist Information Security Assessment Team

Evidence Talks Limited works in close partnership with our team of information security professionals based in our USA Security Horizon facilities in Colorado Springs.

The members of this team all have extensive backgrounds in commercial, United States

Government, and Department of Defense (DoD) environments.

Our INFOSEC offerings include security assessments and network vulnerability evaluations, penetration testing and security policy development.

Internet Crimes Group (ICG)

ICG has unique solutions to problems facing organisations suffering brand diversion, dilution and theft. Evidence Talks founder Andrew Sheldon is a member of the ICG Advisory Board and contributes to the forensic efforts undertaken by ICG.

Using proprietary software and hardware coupled with the enormous talents of its consulting staff, ICG provides unique online investigative capabilities including:

- iThreat™ risk consultancy and mitigation — This may involve one or more of the following services:
- Active corporate security risk assessment
- Active monitoring of critical threats
- Countermeasure consultancy

ICG investigators utilise proprietary technologies as well as public and private data sources to obtain intelligence that clarifies the identity, motives and impacts of individuals or groups.



OUR TRAINING COURSES

OUR extensive experience of performing forensic examinations for the enforcement and corporate sectors since 1993 has brought us into contact with many different situations. Throughout this time, we have been struck by a recurring theme.

In 90% of cases, the evidence we are asked to investigate has already been “damaged” by the actions of the client before we are called in. This can make our job more difficult, time consuming and costly than it would normally be. Therefore we help companies prevent these issues by offering a one day training seminar on Learning How NOT to Damage the Evidence.

Since 2003, hundreds of individuals from a wide and diverse range of companies and institutions have attended our courses, which are universally regarded by those who attend as being of great benefit to them in their jobs and of great value to their companies. They also offer incredible value for money. We run three training courses, either in-house or externally.

Course ONE – Mitigating Business Risk

Course ONE is a high impact one-day training seminar entitled Mitigating Business Risk Using Digital Forensic Practices. It provides delegates with the knowledge they need to protect the evidence in the event of an incident and shows them how to integrate the principles and practices of computer

forensics into the policies and procedures of their organisations.

Course TWO – Building a Forensic First Response

Designed for delegates who have completed Course ONE, this course provides the basic skills and knowledge to allow them to set up a basic digital forensic response capability. All the hardware and software required, plus two days of training on how to use it, are included in the fee.

NSA-Approved INFOSEC Training Courses

The American NSA (National Security Agency) has developed some of the most advanced thinking on information security risk assessment and evaluation methods.

Evidence Talks is very proud to have been appointed by Security Horizon as the only company in the UK authorised to offer NSA INFOSEC training courses, appraisals and accreditations to non-USA citizens in the United Kingdom.

This intensive four-day training course comprises two days on the INFOSEC Assessment Methodology (IAM) and two days on the INFOSEC Evaluation Methodology (IEM). An examination at the end of each course leads to the successful delegate becoming NSA certificated.

OUR TEAM

Andrew Sheldon MSc – Principal Consultant

Andrew is one of the world's leading forensic computing experts, with thousands of investigations under his belt. He holds a Masters degree in Forensic Computing and is a regular speaker at both domestic and international security, forensics and compliance conferences.

Andrew has an in-depth knowledge of PC audit, compliance, desktop management, strategy development, desktop policy and procedures development/review, eDiscovery and eDisclosure issues, internet and PC abuse and risk assessment.



Liam Bateman – Senior Forensic Analyst

Liam has amassed eight years specific expertise in computer forensics combined with significant knowledge and understanding of PC, server and network technologies, risk assessment and analysis, IT security, e-crime/cybercrime investigation and project

management in civil and criminal IT cases. He specialises in the provision of digital forensic services for onsite criminal and civil search orders, both in the UK and internationally, as well as supporting our forensic laboratory. An extremely talented digital investigator.

Richard Peake – Senior Forensic Analyst

An extremely experienced investigator, Richard (Dick) joined Evidence Talks after completing 30 years police service with Bedfordshire Police. The larger part of that was in the Fraud Squad where, in addition to investigating large-scale company fraud,

he was responsible for the management of the computer crime and evidence recovery requirements for the force. Latterly, he set up and ran the Hi Tech Crime Unit for Bedfordshire Police during which time he was a visiting trainer on the National CID Course.

OUR PRODUCTS AND SOFTWARE

OUR experience has helped us to develop some very innovative products for the commercial and enforcement community to assist in the forensic investigation of a number of digital environments.

We are committed to the continued growth of our research and development program and will be releasing a number of new products over the coming year.

Email Forensics

As a leading forensics practice, we have been performing forensic analysis of email systems since 1993. Frustrated by the lack of tools that do what we wanted, we decided to write our own. The result is LoPe™ which stands for Lights Out PST Extraction.

LoPe

- Quickly and forensically extracts all email messages and attachments from multiple PST files
- Fully automatic — no need to process individual PST files by hand
- Unlimited number of PST files can be processed automatically
- Recreates the internal PST folder structure



- Extracts all message headers and properties — even things other tools can't see!
- Export in MSG, EML or XML format — output can be viewed in a browser
- Full audit trail for every action
- Every message and attachment is hashed
- Command line interface, thus LoPe can be easily batch scripted
- XML output format is fully customisable using XSL style sheets

Whether you have five or 5,000 PST files to export, whether the driver is a forensic investigation, Sarbanes Oxley (SOX), FSA, FCC, SEC or other regulatory, legal or

consensual request, the disclosure of email is something that should be performed using appropriate, trusted tools and procedures. We believe LoPe will save you considerable time and effort.

LoPe Assistant™

Reviewing email for keywords and relevance is a daunting task and one that takes time and considerable effort. But it's all about to get easier with the introduction of LoPe Assistant.

Having forensically extracted messages from PST files, LoPe Assistant helps you review, search, tag, filter and export the results you want. Using an intuitive interface, LoPe Assistant can dramatically cut the time and effort needed to perform email analysis. And it does not stop there.

Delivery of email analysis results to non-technical third parties has always been problematic. Creating a special PST or providing individual messages in MSG or EML format is far from ideal as there can be issues if these data files are viewed on systems that have an internet connection. Also, these formats lack the level of detail required for true forensic analysis.

Because LoPe can output the raw message data from a PST in XML format, LoPe Assistant can be used to perform detailed analysis and review and can be re-distributed to third parties in order that they

can further search and review the results, avoiding the need to use standard email clients to view forensic data.

Even better, LoPe Assistant can be used to deliver compelling, data rich results in a format that can be imported by most leading document management systems.

LoPe Assistant has the following features:

- Understands the XML output from LoPe and provides a familiar view of the data
- Provides comprehensive SEARCH, TAGGING, FILTERING and EXPORT functions
- Quickly review thousands of messages and select the ones you want
- Powerful Boolean search functions
- TAG messages as NORMAL, IMPORTANT, PRIVATE, PRIVILEGED or custom tag
- FILTER your view of messages based on TAG attribute
- EXPORT messages in XML format based on search or tag criteria
- Maintain full evidential traceability to the source of each message
- FREE re-distributable results viewer

Remote Forensics

OVER the last few years the number of corporate investigations requiring a forensic response has exploded, driven by increasing use of technology and a dramatic rise in the number of internal and external threats.

When incidents do happen, the need to preserve digital evidence prior to an investigation is often overlooked, with the result that proper investigation is either compromised or restricted in scope.

All too often the first thing the investigators do is to 'have a quick look' at the suspect's computer to establish if there is anything of interest present. At the least, this will result in tainting of any potential digital evidence and, at the worst, can obliterate any shreds of evidence that were present.

Ideally, every office should have the capability to respond to incidents involving potential digital evidence in a timely and knowledgeable manner. Unfortunately, having staff with appropriate skills and forensic equipment in the right place at the right time is a costly option.

No matter if the incident is desktop abuse, theft of intellectual property or a hacking incident, you need to protect the evidence and you need forensic investigation skills on site in a hurry.

The concept behind the Remote Forensics solution is simple:

Our clients need to react faster and smarter to digital incidents, so we've designed a forensically-sound environment which allows us to be 'on site' anywhere in the world at the press of a button, performing all the usual forensic tasks of imaging, analysis and reporting.

Based on tried-and-tested enterprise grade server hardware, our remote forensics 'POD' combines a formidable suite of forensic tools with highly secure communications to enable a very effective 'remote hands' forensics facility. This allows a forensic expert based anywhere in the world to perform forensic imaging and analysis of digital media at local speeds via our secure network.

By itself, the capability of the POD is impressive but that's not the whole story.

When an incident occurs, one of the most significant factors leading to a successful investigation is a structured investigation methodology. To support this, Evidence Talks have developed an end-to-end Forensic Incident Management Service™ (FIMS™) which is supported internationally by a growing network of Forensic Service



Partners (FSPs) who can be remotely 'on site' within minutes.

Existing solutions to the problem of enterprise-wide forensic incident response tend to focus on accessing targeted systems via the corporate network. This naturally means that there must be network connectivity to the suspect machines and usually involves installing a 'client' application on to every machine you might want to investigate before an incident.

The more traditional approach has been for the corporate to call on the services of a forensic team who can mobilise to the problem sites quickly. Once on site, the general methodology is to identify target systems, remove the hard disks and create forensic images using standard tools and write-protection techniques.

There are problems with both the above scenarios.

Deploying forensic client software on an enterprise-wide basis is not a task to be undertaken lightly. Multiple desktop builds will likely exist and the forensic client will need to be integrated with each one.

Likewise, pushing the client to target machines in the heat of an active investigation may not be possible — through lack of network connectivity — or desirable because of bandwidth or privacy issues. It is for this reason that most large-scale enterprises still prefer to mobilise a forensics

team to the site of an incident where control is exercised over the digital environment and, if forensic images are required, they can be taken in the traditional way.

It was with these issues in mind that Evidence Talks developed our Remote Forensics solution comprising three core elements:

- Remote Forensics POD — used to receive digital media
- FIMS system — Internet/Intranet based Forensic Incident Management System
- FSP network — Global providers of forensic expertise

Enterprise clients who recognise the need to respond quickly, efficiently and in a forensically-sound way to incidents in multiple locations place a POD in each of their key risk locations.

The PODS are simply placed in a convenient rack space and given a connection to the Evidence Talks global VPN. There is no requirement for the PODS to access the corporate networks and no software is installed on any other computers. In effect, the PODS are a standalone forensic facility.

- For a fully detailed description of how the system works and technical specifications, please consult our Remote Forensics brochure.

0845 125 4400

www.evidencetalks.com

info@evidencetalks.com