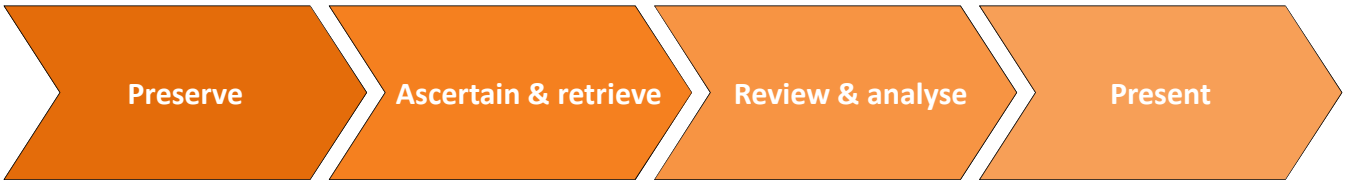
SHINEWING Forensic and Investigation Services

Technology is the predominant business tool of today, SHINEWING's **Forensic and Investigation Services** team can provide innovative and tailored computer forensic services……



Our team can do...

For solicitors / counsel

- **Forensic acquisition** of electronically store data
- Digital evidence **restoration**, **undeletion**, **filtering**, and **analysis**
- **Electronic evidence** collection procedures review
- **Cross-examination** and visual **presentation**
- **E-discovery** for multi-language support

For corporations / financial institutes

- **Incident response** consultation
- **Regulation compliance** and **corporate policy** review
- E-transaction **tracing**, **analysis** and **interpretation**
- Digital evidence **recovery**, **preservation**, and **authentication**
- **Fraudulent activities** investigation
- **Expert witness** support
- **Password** recovery
- Permanent data **deletion**

We can respond quickly...

We recognise that critical evidence residing in digital media is usually volatile. The ability to respond quickly to an incident is extremely important in any type of computer forensic work. Therefore, our team is committed to providing an immediate response to requests once such engagements are formally confirmed. We will be able to travel (local and international) at short notice, with a full range of specialist forensic equipment, to any target location(s) within the region to acquire evidence and conduct on-site examination. Alternatively, we can analyse any acquired evidence in our in-house forensic laboratory. Preliminary results or deliverables can be made available within a short period of time.

SHINEWING Forensic and Investigation Services

Questions and answers on Computer Forensics …

What is Computer Forensics?

Computer forensics involves preserving, recovering, analysing and presenting electronic evidence pertaining to legal evidence stored on a digital storage media, which can be submitted to a court of law as evidence.

What evidence can be found in a computer / computer system?

Potential electronic evidence includes:

- active and deleted files
- graphics, audio and video
- email correspondences
- Internet activities and browsing history
- illegal downloads
- user-defined settings and recently accessed/modified files
- outbreaks of viruses and unauthorised access
- hardware and software configuration, etc.

Who needs Computer Forensics?

- Companies suffering from (alleged / suspected) fraud or security breach by internal or external parties or seeking ways to monitor work flow and business processes
- Professionals or parties engaged to investigate fraudulent or illegal transactions, e.g. money laundering
- Individuals and organisations requiring recovery or extraction of forensically sound evidence from digital media for inquiry, negotiation and litigation
- Law enforcement agents seeking evidence to support litigation against offenders
- Solicitors and counsel, in the process of e-discovery and when expert witness evidence is sought

"We received a report of corporate malpractice in our organisation from an anonymous whistleblower. We are not sure who is involved and the extent of such report is valid. What can we do?"

Identifying prime suspects and filtering critical electronic evidence are always a challenge but is utmost essential in any type of investigation. Unstructured investigation will not only disrupt business operations, most likely it will delay, overlook and even destroy critical evidence. Our Computer Forensics specialist can investigate and identify the potential offenders and the extent of the violation in a timely and confidential manner, allowing management to make proper and informed decisions, often under very demanding circumstances.

SHINEWING Forensic and Investigation Services contacts

Anita Hou
Partner
Tel: +852 3909 8968
Email: anita.hou@shinewing.hk

Matthew Chu
Senior Manager
Tel: +852 3909 8917
Email: matthew.chu@shinewing.hk