


**Quizzes 英语小测验**
**ABOUT CHONGQING**
**Government Constitution**
**Leading Officials**
**Friendship Cities**
**History**
**Mayor's Mailbox**
**THREE GORGES**
**Introduction**
**Sceneries**
**Route map**
**CHONGQING TODAY**
**Economy**
**Investment Policies**
**Education**
**Medical Care**
**Travel**
**Transportation**
**Culture and Art**
**DISTRICTS & COUNTIES**


## "Digital Detective" To Attack Global Cyber-Criminals

2007-08-15 15:50



*Tracking down crime: once alerted, computer investigators can use innovative, fast software to probe suspected criminals' hard drives - anywhere in the world - without having to go to the site or take suspect disks to a lab.*

THE Internet has become the medium that many criminals are using to perpetrate crimes. Because it pervades all aspects of most of our lives these days, it also touches many, if not all, areas where incidents can occur.

Every year, companies spend vast sums getting software security staff to investigate incidents at branch office before they can even start investigating computer crimes. Imagine the cost involved should these firms have multiple sites spread over a wide geographical area, possibly across a country or a continent.

Now, a unique new weapon in the war against cyber-criminals has been launched by forensic computing experts in the United Kingdom. It is called Remote Forensics and allows specialist investigators to respond much faster, reducing valuable time that could allow criminals to cover their tracks.

The groundbreaking software allows "digital detectives" to investigate suspects' hard drives anywhere in the world without having to travel to the site or transport the suspect disk to the lab.

On being alerted at work, at home, in a park - almost any place - a forensic computing expert can track down the criminal's hard drive.

expert could use the remote system to start investigating the contents of a system used by suspected paedophile, identity thief or fraudster on the other side of the globe.

As long as the forensic analyst can connect to a network, even wireless or 3G, he or she can securely preserve and analyse any digital media at almost the same speed as if they were sitting at the suspect's own computer.

The system is set to revolutionise the way that multinational companies such as banks can investigate computer crime within their global networks, by eliminating the time and cost involved in sending investigators to the scene of a far-away digital incident.

The anti-cyber-crime system is produced by the Evidence Talks company, described as one of the most highly regarded digital forensic consultancies in the UK.

The company's managing director Andrew Sheldon said: "Major companies and businesses are buckling under the onslaught of attacks from computer criminals exploiting security weaknesses in their networks.

"It can take only seconds for valuable intellectual property such as pharmaceutical formulas, business plans and secret designs to be spirited away over the Internet, causing untold damage to businesses' profits, brand and reputation.

"Speed of response is vital in detecting and prosecuting culprits before the digital clues they leave behind are damaged. Until now, the only solution has been to have a forensic computing expert at every location or be prepared to dispatch a team anywhere in the world at the first sign of trouble. With Remote Forensics, businesses can react instantly, saving precious time and money."

Remote Forensics consists of two main components, a hardware pod that is installed at a company's remote risk locations, and FIMS (forensic incident management service), a full secure case-management application that can be operated over the Internet. The customer's data stays on site ensuring its information is secure at all times.

After suspicious activity is detected, a local IT resource loads the suspect media into the pod and grants access to the forensic computing expert. No software is installed on clients' systems, no client data is transferred over the Internet and there is no effect on their normal business activities.

The FIMS generates all case paperwork and automatically records and logs all actions taken, ensuring that results of the investigation are evidentially sound at every step of the way.

From identifying the data to be captured, through to providing expert witness services in court, Evidence Talks has been serving the companies and organisations of the world with digital forensic and computer forensics expertise since 1993.

"Digital data can be found in a variety of mediums including hard disks, CDs, mobile phones and PDAs, email systems and servers including network attached storage (NAS) and storage area network (SAN) technologies," said a spokesman. "Typical cases include IP theft, fraud, identity theft, email abuse and inappropriate content. In fact, with thousands of investigations under our belt, we cover the entire spectrum of computer forensics and digital crime.

"We can provide a comprehensive range of covert Internet investigation and analysis including email analysis and packet capture, web profiling, identity determination, posting visibility monitoring, domain control mapping, IP intelligence services, Internet risk/threat mitigation, brand dilution and diversion and more. Every case where computer forensics is involved is examined and progressed in accordance with the Association Of Chief Police Officers' guidelines and results delivered in clear, factual and easy-to-understand reports."

Cyber crime can range from a blackmail email to a full credit-card fraud. Experts say t

many people are not taking all the precautions they should to protect themselves and their organisations from viruses, trojans and other Internet-based malware.

Evidence Talks has many years of experience and knowledge working and detecting area of digital crime and, in addition, can offer consultancy services to harden systems after an incident.

The company also has access to unique tools that aid the gathering of evidence and intelligence, making Evidence Talks the primary source for specialist Internet investigation in Europe.

Its staff are fully trained and experienced in the use of a wide range of forensic tools and utilities, and they work to the latest standards for digital evidence handling, reporting and analysis. Its principal consultant has a master’s degree in forensic computing and teaches a module on a similar degree course.

Before joining Evidence Talks, its analysts have worked as network engineers, Fraud police officers and management consultants. A combination resulting in its clients benefiting from a broad range of experience, drawn from different backgrounds. (Source: British Consulate-General in Chongqing)

[中文译文 \(Click to read the Chinese Version\)](#)

editor : 龙华

[related news:](#)

---

Chongqing Daily News Group | Site Guide | Contact Us

<http://www.cqnews.net/> All rights reserved

Reproduction in whole or in part without permission is prohibited

Address:F6,126#Yuzhoulu,Hi-tech District,Chongqing Zip code:400041

Fax : 023-68577897 E- mail:info@cqnews.net