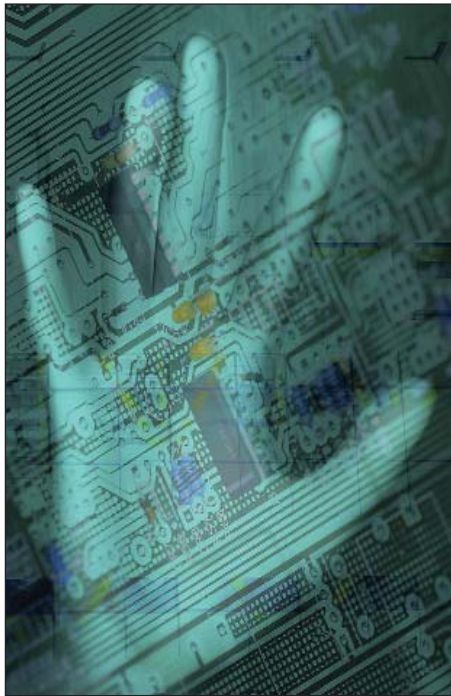


St. Louis Technology News

THE TECHNOLOGY SPIRIT OF ST. LOUIS™

TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH

Admissible Evidence



Computer forensic techniques ensure that data collected during electronic discovery can be used as evidence in a court of law.

On TV, crime scenes are typically filled with people — uniformed officers, detectives and others interested in the investigation. While that may make for good drama, it could potentially damage a real-life case. Activity within the crime scene can destroy sensitive physical evidence and hamper the investigation.

The same holds true for electronic evidence. Electronic evidence must be

carefully preserved so that computer forensic investigators can do their work.

“In fact, electronic evidence is in many ways more complex than physical evidence,” said Ispirian CEO Tom Smith, a forensic scientist and a member of the American College of Forensic Examiners Institute of Forensic Science. “While it’s easy to touch, see and photograph physical devices, it’s obviously impossible to do that with file systems and other residual data. Electronic evidence can easily be tainted without proper handling practices.”

Chain of Custody

The processes that help preserve electronic evidence can be summed up in the term “chain of custody.” First, the computer forensic investigator must gain possession of the electronic media

continued on page 2

St. Louis Technology News

PRSR1 STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146



Admissible Evidence

continued from p. 1 ...

with proper authority. The owner of the data must voluntarily surrender the data, or a court order or subpoena must be in place.

Next, the investigator must make sure that no damage is done or change is made to the original media. Something as simple as turning on a computer can alter the file system and render the evidence useless in a court of law.

“Evidence is preserved by the application of sound chain-of-custody processes,” said Smith. “The chain of custody in electronic discovery is not just the starting point of every case — it’s the backbone of every case. It is potentially the most crucial element that will support the ultimate findings.”

Preserving the Data

The chain of custody includes both the physical devices themselves and the electronic evidence potentially stored on them. As with physical evidence, special handling and preservation practices are used to reduce the risk of tampering or destruction.

However, computer forensic

investigation techniques go further due to the nature of electronic evidence. In the field, the Ispirian team uses special gloves, grounding, and storage and shipment containers to prevent damage by electrostatic discharge. The scene is documented, and all investigative activities and evidence are carefully logged.

In the lab, the Ispirian team builds its own workstations using special disk controllers and hard drives that allow data to be copied from the suspect computer without altering it in any way. Locked cages and fire-proof vaults are used to protect against theft and other hazards.

“In an increasing number of cases, it’s not possible to seize the actual equipment,” Smith said. “In those cases we create a media image at the scene for off-site analysis. Nevertheless, strict chain-of-custody processes must be followed.”

Following the Rules

All of this effort has one goal — to ensure that the electronic evidence can be used in court. Computer forensic investigators must be able to certify the authenticity and integrity of the data to meet evidentiary rules.

“The evidence itself is almost

never questioned — it’s difficult to deny allegations that are spelled out in the data,” Smith said. “However, opposing counsel will often challenge the authenticity of your data or claim a broken chain of custody. That’s why your IT staff should not be the ‘go-to’ resource for this critical aspect of electronic discovery. They simply don’t have the necessary tools and training to collect electronic evidence.”

Many computer forensic investigations occur outside the realm of law enforcement to support or defend against civil lawsuits, or to meet regulatory requirements. Although a wrongful discharge or theft of intellectual property claim may not involve the same kind of “crime scene” as a murder, evidentiary rules still must be carefully followed.

“One of the cardinal rules of computer forensics is to treat all investigations as though you were going to refer the case to law enforcement,” said Smith. “We first clear the scene and don’t allow anyone in the area until the investigation is complete. We then follow a precise set of procedures to ensure that the evidence we collect can be used in a court of law.”