WASHINGTON, August 16, 2002 (source: http://www.cbsnews.com/stories/2002/08/16/tech/main518981.shtml)

Gathering The E-Evidence

In The E-Mail Age, Scraps Of Conversation Are Everywhere

By Connie Cass

(AP) Not since the glory days of letter-writing, before the advent of the telephone, have people committed so much revealing stuff to written form as they do in the age of computers.

All those e-mail messages and electronic files are a treasure trove of evidence for law enforcement officers, whether they are targeting terrorists, crooked CEOs or local drug dealers.

The challenge for police and prosecutors is learning how to dig up and preserve these electronic gems.

"Any agent can come in and look through papers, but not every agent can do a thorough computer search," said David Green, deputy chief of the Justice Department's computer crime section, which helps train federal and state investigators.

Green teaches that a mistake as simple as turning off a computer can wipe away valuable evidence. Knowing such basics, and the ins and outs of privacy law, is essential when electronic evidence may play a role in so many cases.

"It's like the gift that keeps on giving," said Tom Greene, a deputy attorney general in California, one of the states suing Microsoft Corp. in an antitrust case built largely on computer messages. "People are so chatty in e-mail."

E-mail revealed the shredding of documents at Arthur Andersen, and exposed Merrill Lynch analysts condemning stocks as a "disaster" or a "dog" while publicly touting them to investors.

Anti-American sentiments in messages Taliban fighter John Walker Lindh and shoe bomb suspect Richard Reid sent to their mothers were gathered as evidence against them.

And when Wall Street Journal reporter Daniel Pearl was kidnapped and killed in Pakistan, investigators used e-mails from his abductors to track them down.

When drug dealers are arrested, police search their electronic organizers and cell phones for associates' names and telephone numbers. When someone is accused of molesting a child, his computer is searched for child pornography. When a company is sued, it can be forced to turn over thousands of employee messages.

"E-mail has become the place where everybody loves to look," said Irwin Schwartz, president of the National Association of Criminal Defense Lawyers.

One reason is that computer data is difficult to destroy. Just clicking "delete" won't do it, as Oliver North learned during the 1980s Iran-Contra probe, one of the earliest investigations to rely on backup copies of electronic messages.

Deleted files can linger, hidden on a computer's hard drive until that space is overwritten with new information.

"The best way to get rid of computer data is to take the hard drive and pound it with a hammer and throw it in a furnace," said John Patzakis, president of Guidance Software, which makes forensic software that helps police find hidden files.

Even that might not work with e-mail, which investigators may also be able to track down in an employee's office server, stored by Internet providers, or in the recipient's computer.

To go hunting through computer data, law officers need a search warrant issued by a judge. Winning legal permission to eavesdrop on e-mail as it's transmitted is more difficult, because that is considered the same as wiretapping a telephone. Investigators generally need a court order based on probable cause that the wiretap will reveal evidence of a felony.

Criminals, or people who simply want to protect their secrets, can use encryption software to scramble their e-mail. And special software can overwrite computer files, so they are truly deleted. Most criminals aren't that savvy yet, prosecutors say.

Even law officers make the mistake of indiscreet e-mail. Defense attorneys commonly scour messages between police or prosecutors to look for ammunition to question investigative techniques or suggest bias. Or, one of the prosecution's expert witnesses may have posted notes on the Internet that contradict his testimony.

Every U.S. attorney's office across the country has a computer and telecommunications coordinator, and the Justice Department is pushing more of its prosecutors to take cybercrime courses. The department also finances some training for state and local law enforcement.

"The problem is the uninitiated police officer who will go in and turn on a computer to look to see if it's worthwhile to send the computer in for examination," said Peter Plummer, assistant attorney general in Michigan's high-tech crime unit.

"When you boot up a computer, several hundred files get changed, the date of access, and so on," Plummer said. "Can you say that computer is still exactly as it was when bad guy had it last?"

A defense attorney could argue it's not, and try to convince a jury that evidence has been mishandled or tampered with.

When feasible, investigators usually prefer to use special software to make an exact copy of the contents of a computer's hard drive. This can be done without even turning on the computer.