

## A Criminal Observation

*In the fight to find, arrest and prosecute online criminals, the Perry Township Police Department in Massillon, Ohio uses Expert Observer® to perform third-party identity verification and capture illegal behavior.*

### Rising Illegal Activity

According to an October 8, 2003 report by the National Society for the Prevention of Cruelty to Children, more than 20,000 images of child pornography are posted on the Internet every week.

Around the country, multi-jurisdictional task forces are successfully investigating and arresting those that attempt to exploit children online. In addition to performing his job responsibilities as a patrol officer, Officer Pete Gessford is a member of one such task force at the Perry Township Police Department in Massillon, Ohio.

"The Internet has made it easier for the bad guys to commit their crimes," said Gessford. "While the common pedophiles or molesters used to risk exposure when he/she watched children at the playground, they now have a certain factor of anonymity when committing the same crime online. Our goal is to stop that."

### Going Undercover

The taskforce uses three methods to find and arrest these violators. The first is by entering chat rooms and posing as children in hopes of seeking out offenders. The second method involves identifying the IP address of individuals distributing child pornography over the Internet on corporate networks. Third, the taskforce reviews files provided by the IT departments of organizations where a user is suspected of illegal activity.

In 2003 the Crimes Against Children Research Center at the University of New Hampshire published a report entitled "Internet Sex Crimes Against Minors: The Response of Law Enforcement." This report reviewed online victimization cases that occurred from July 1, 2000 to June 30, 2001. The study found that US law enforcement has made an estimated 2,577 arrests in the 12 months after July 1, 2000 for Internet sex crimes against minors. Undercover law enforcement officers posing as minors contributed to 25% of those apprehended.

"First, we assume the role of a child and begin chatting with these subjects," said Gessford. "Once a level of trust has been established, we push to set up a physical meeting so that an arrest can be made."

### Dissecting Internet Behavior

In addition to making arrests, another aspect of Gessford's role is to gather evidence. This could mean capturing IP addresses over the Internet or viewing packets provided by companies with users suspected of illegal activity. Like many government entities, the department has limited resources and limited budgets. Despite these setbacks, Gessford seeks out the latest technology tools, including a network analyzer, to gather the necessary evidence to prosecute criminals.

"I take a more active role in tracking down file servers on the Internet," said Gessford. "I log into the servers and download the suspected child pornography, issue a subpoena to the ISP and then execute a search warrant on the suspect's computer. Pedophiles are becoming more and more clever. They utilize the same mediums as those that pirate software (warez) and music. We are seeing servers utilizing Kazaa, IRC, FTP, FSERVs, etc."

During a company investigation, Gessford came across Network Instruments' Observer®, a multi-protocol, distributed network analyzer used by IT administrators to monitor, troubleshoot and manage their networks.

"I was working on a local case where an employee of a local business was abusing the network policies of his company to chat in suspected pedophile chatrooms," said Gessford. "The IT department used Observer and caught on to his activity. They captured all Internet activity using the Observer program and then turned the captured data over to us. We didn't have a client that could read this easily, so we asked for help from Network Instruments."

### Uncovering Clues With a Network Analyzer

To assist with the case, Network Instruments supplied a copy of Observer to the department. Observer is a network analyzer designed for IT administrators that require complete network visibility. With features such as packet capture and decode, real-time statistics, error tracking, triggers and alarms and advanced filtering techniques, Observer has helped thousands of administrators worldwide troubleshoot, monitor and maintain corporate networks and systems. Gessford uses Observer to review packet capture files ascertained from corporate IT departments that may suspect employees of illegal activity.

"I realized with Observer's packet capture, we could collect information we required for our investigation much easier," said Gessford. "Many programs now mask the IP information of the end user and we need to find out which ISP we must subpoena for user records. Where we once had to subpoena the software company (ex. Yahoo Chat) to figure out the IP Address of the user, which was time-intensive and costly, now we can "packet sniff" the chat conversation and get the IP address directly."

*In summary...*

### About Perry Township Police Department

The Perry Township Police Department serves a population of over 31,000 in Stark County, Ohio. In addition to patrolling the streets and protecting the community, the department offers many citizen programs including the Community Anti-Terrorism Training Institute (C.A.T. Eyes), Drug Abuse Resistance Education (D.A.R.E.), School Resource Office Program, Citizen's Police Academy, Bike Patrol and Crime Watch. The Department has also established an Electronics Crime Section, which works with state and federal agencies to investigate, apprehend and prosecute Internet sex crimes, particularly those committed against children and youth.

### Challenge

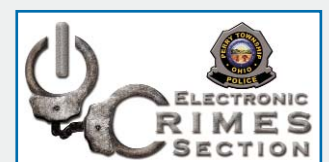
While the Internet has offered many advantages it has also given child molesters and pedophiles a greater level of anonymity and privacy. The Electronics Crime Section at the Perry Township Police Department is a member of a multi-jurisdictional task force dedicated to finding and apprehending online sex offenders. The investigations require advanced network visibility solutions to identify and verify illegal online activity. Officer Pete Gessford needed a method of determining an offender's IP Address and reviewing files obtained from organizations that suspect illegal employee activity. Gessford sought a tool to decode packet captures, identify IP addresses and offer an additional level of integrity while gathering evidence.

### Solution

As part of an online pedophile investigation, IT administrators at a nearby corporation introduced Gessford to Network Instruments' Observer. He immediately recognized that a network analyzer was the investigative aid his job required. With Observer, Gessford can quickly decode captured files and identify IP addresses masked by popular file-sharing programs. While surfing online, Gessford uses Observer to capture transferred packets and confirm results. Gessford found not only a solution that is intuitive and easy-to-learn, but also one that can gather and present credible evidence to convict online offenders.

**"I realized with Observer's packet capture, we could collect information we required for our investigation much easier."**

**Pete Gessford  
Patrol Officer  
Perry Township Police Department**



### Releasing Convincing Evidence

Using Observer has not only saved Gessford time in locating evidence, but offers him additional credibility when presenting the evidence of child pornography in court. Freeware, like Kazaa, could provide the IP address, but in cases where the illegal activity was transmitted via a freeware application, the reliability of such data is questioned. Observer, a third-party application, designed solely to perform independent, passive views of network traffic offers greater authority.


"My data stands up better when I explain I found the information with Observer," said Gessford. "It is more credible to the jury to explain I used Observer rather than saying my freeware Kaaza, which provides millions of people ways around copyright information, gave me the information."

Gessford uses Observer to locate and confirm IP Addresses as well as log packets. During online investigations, Gessford has Observer capturing packets and keeping a record of all online activity. When a suspect is sighted, Gessford can review Observer's data, which has already captured the IP address, web address and type of file that was transmitted.

"I not only use Observer during chat conversations but also to capture packets that are sent back and forth when I log into a suspected server," said Gessford. "I have Observer installed on my undercover computer and use it to verify or confirm that the peer-to-peer software is giving me valid results. I also use Observer to discover IP Addresses that are often hidden by file sharing systems."

### Network Training for a Street Cop

Over time, Gessford has learned to use Expert Observer to securely and accurately gather evidence of criminal activity to successfully prosecute pedophile cases. He appreciates Observer's ease-of-use. As a patrol officer, with countless responsibilities, Gessford required a program that could quickly aid in gathering evidence without having to spend countless hours learning a new application.

"I'm a street cop, not a network guy," said Gessford. "Even then, I found Observer easy to use. The packet capture capabilities and filtering techniques are what I use the most. The product is excellent. It's saved time, provided credibility and ultimately played a part in bringing pedophiles and molesters to justice." 

"My data stands up better when I explain I found the information with Observer."

-Officer Pete Gessford

### About Packet Capture and Decode

Observer offers complete real-time packet captures and decode at wire speeds at any local or remote location. Packet capture displays show total traffic, captured traffic and dropped packets (if any). View captured traffic packet-by-packet according to specific filter criteria you define. After a capture is complete, Observer allows for post-capture filtering to isolate only the pertinent information. Observer's protocol decodes now number well over 500, and over 4000 unique frame types are identified. For switched segments, Observer offers capture on any one port (or group of ports depending on your switch) without leaving the Observer interface to set up the switch. Observer also supports multiple simultaneous captures from a single console. Up to 64 concurrent captures are supported from adapters located on the local system. Additionally, an unlimited number of simultaneous concurrent captures are supported from remote Probes. Multiple sessions also support multiple concurrent statistic collections.

### About Expert Analysis and Real-Time Expert

Observer's Real-Time Expert collects critical events; breaks down conversations into subprotocol groups and instantly identifies problems as they happen. The Expert Summary Problem Analysis shows all error events in a single concise display. Further analysis, including cause of errors, can be obtained on any connection-orientation problem with a simple drill-down. Observer currently monitors over 500 network conditions, including 50 specific to wireless.

### About Network Instruments

Networks Instruments is the industry leading developer of distributed, user-friendly, and affordable network management, analysis and troubleshooting solutions. The award-winning Observer family of products combines a comprehensive management and analysis console with high-performance Probes to provide integrated monitoring and management for the entire network (Ethernet, Gigabit, Wireless, and WAN). All Network Instruments products are designed utilizing Distributed Network Analysis (NI-DNA™) architecture. With NI-DNA, the Observer solution set simplifies network troubleshooting and management, optimizes network and application performance and scales to meet the needs of any organization. Founded in 1994, Network Instruments is headquartered in Minneapolis, Minnesota with offices in London, Paris and throughout the USA with distributors in 50 countries. More information about the company, products, innovation, technology, NI-DNA, becoming a partner and NI University can be found at [www.networkinstruments.com](http://www.networkinstruments.com).

**Corporate Headquarters** Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA  
toll-free: (800) 526-7919 • telephone: (952) 358-3800 • fax: (952) 358-3801 • [www.networkinstruments.com](http://www.networkinstruments.com)

**European Office** Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom  
telephone: +44 (0) 1959 569880 • fax: +44 (0) 1959 569881 • [www.networkinstruments.co.uk](http://www.networkinstruments.co.uk)

**France, Italy and Spain** Network Instruments • 1 rue du 19 janvier • 92380 Garches • Paris • France  
telephone: +33 (0) 1 47 10 95 21 • fax: +33 (0) 1 47 10 95 19 • [www.networkinstruments.fr](http://www.networkinstruments.fr)

