



# Computer Forensic Investigations

## **Computer Forensic Services, LLC**

**Michael Barba, CPP**  
**Partner**

732-263-0676  
mbarba@computer-forensic.com  
www.computer-forensic.com



# Topics to be covered

- *Tools: Hardware and Software*
- *Procedures for protecting electronic evidence*
- *Acquiring Electronic Evidence*
- *Evidence Analysis and Data Recovery*

# Computer Operating Systems





# Computer Forensics Defined

- ◆ "Computer Forensics deals with the preservation, identification, extraction and documentation of computer evidence."\*
- ◆ "Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact."\*
- ◆ Recovering Information the naked eye can no longer see.



# Computer Forensic Example

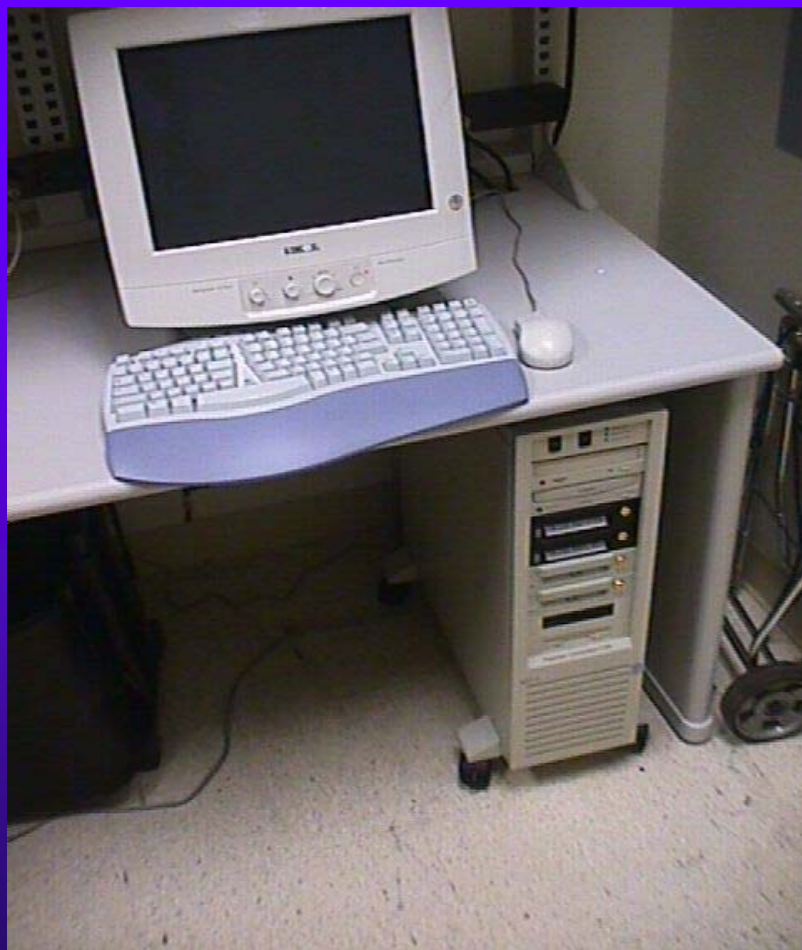
- ◆ Recovery of over 1000 E-Mails off of a hard drive.
- ◆ A year and half after the individual left the company.
- ◆ After the hard drive had been formatted
- ◆ After the machine was in use by another user for that year and a half
- ◆ "Best way to remove e-mail from a hard drive is to hit with a sledge hammer and throw it into a furnace." John Patzakis, President & Chief Legal Officer Guidance Software



Tools

The Hardware

# Some of the Equipment- The Tower

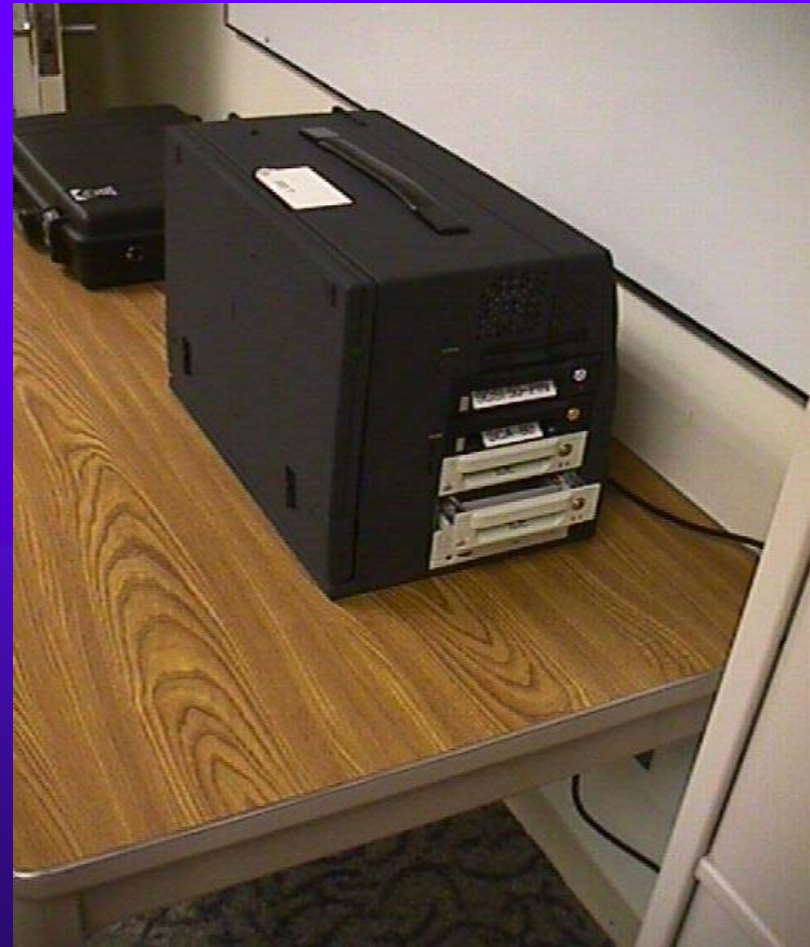


# More Equipment- The Image Master





# Portable Equipment??



# The Workhorse Unfolded



Now This is Portable!!



# The AirLite Unfolded:



# Some Peoples' Tool of Choice





Tools

The Software

# Some of the Software



**The Norton Utilities®**  
for Windows/DOS

**SYMANTEC®**

**Disk #2 – Emergency/  
Data Recovery**

The Norton Utilities, Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. ©1994 Symantec Corporation. All Rights Reserved. Printed in the U.S.A.  
07-50-01164 109-125-17 2/94

**1.44 MB Diskette**

The image shows the packaging for the Norton Utilities software. It features a white box with a yellow header and a black footer. The text on the box reads "The Norton Utilities for Windows/DOS" and "SYMANTEC". Below this, it says "Disk #2 – Emergency/ Data Recovery". The bottom of the box contains the Symantec logo and the text "1.44 MB Diskette".

**Encryption  
Linux  
Boot Disk**

Disk  
1/2

2075 NORTHEAST DIVISION  
GRESHAM, OREGON 97030  
PHONE: (503) 661-6912  
WWW.FORENSICS-INTL.COM

**ni** New Technologies Inc.  
THE ULTIMATE IN COMPUTER FORENSICS

For NITL Customers Use Only.  
Copyright is the exclusive property of NITL.

The image shows the packaging for the Encryption Linux Boot Disk. It features a white box with a black header and a black footer. The text on the box reads "Encryption Linux Boot Disk" and "Disk 1/2". Below this, it says "2075 NORTHEAST DIVISION GRESHAM, OREGON 97030 PHONE: (503) 661-6912 WWW.FORENSICS-INTL.COM". The bottom of the box contains the New Technologies Inc. logo and the text "THE ULTIMATE IN COMPUTER FORENSICS".

Version 2.18

**SafeBACK®**

MICHAEL BARBA

Licensed For Use By:

**ni** New Technologies Inc.  
THE ULTIMATE IN COMPUTER FORENSICS

2075 NORTHEAST DIVISION  
GRESHAM, OREGON 97030  
PHONE: (503) 661-6912  
www.forensics-intl.com

The image shows the packaging for the SafeBACK software. It features a white box with a black header and a black footer. The text on the box reads "Version 2.18" and "SafeBACK". Below this, it says "MICHAEL BARBA" and "Licensed For Use By:". The bottom of the box contains the New Technologies Inc. logo and the text "THE ULTIMATE IN COMPUTER FORENSICS".

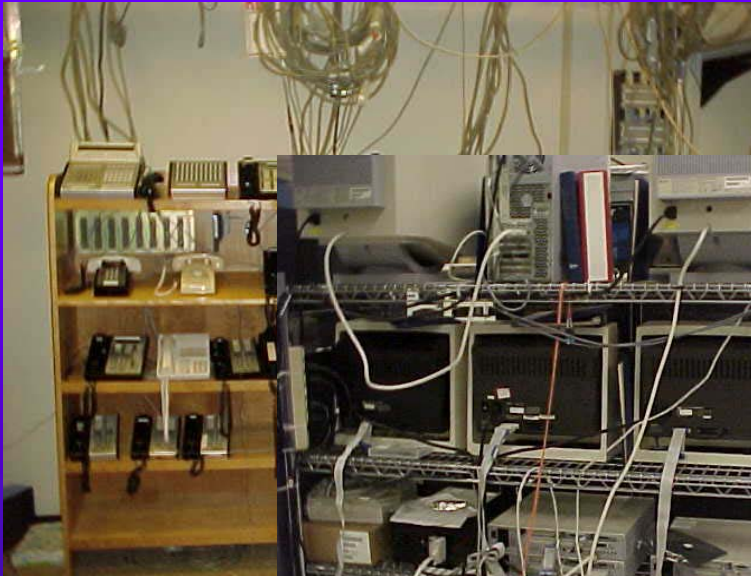


# Procedures

## Protecting Electronic Evidence



# Label Everything!





# Some Questions to Ask

- ◆ Was the computer system instrumental in the offense, i.e., a hacker or harassment case?
- ◆ Is the computer being used to store evidence of a crime, i.e., drug dealer maintaining trafficking records?



# Secure the Computer as Evidence

- ◆ Photograph and log room, position of computer and status of computer.
- ◆ If the computer is "OFF," Do Not Turn "ON."
- ◆ If the computer is "ON," Do Not Turn "OFF."
- ◆ Huh??
- ◆ Place Evidence tape over each drive slot
- ◆ Photograph and label back of computer components while they are plugged in.
- ◆ Label all connection ends to allow reassembly if needed
- ◆ If transporting, treat all components as fragile
- ◆ Collect all devices such as cables, keyboards and monitors
- ◆ Collect instruction manuals, documentation, and notes
- ◆ User notes may contain passwords



# Prepare Evidence and Chain of Custody Forms

- ◆ Evidence Form

- Log make, model, and serial numbers
- Copy stays with evidence at all times

- ◆ Chain of Custody

- Who, What, Where, When, Why, How
- Copy stays with evidence at all times



# Acquiring Electronic Evidence

# The Hard Drive

- ◆ Forensic Image of the hard drive means to take an exact copy of a hard drive including deleted files and areas of the hard drive that a normal backup would not copy.
- ◆ Never boot off of the hard drive
- ◆ Use write protection software to protect the original evidence.
- ◆ Make a copy of the original evidence and do all work off of the copy
- ◆ Document all aspects of the hard drive.
- ◆ Tag and store original evidence
- ◆ Best evidence is original evidence.





# Evidence Analysis and Recovery

# Where Should One Begin?

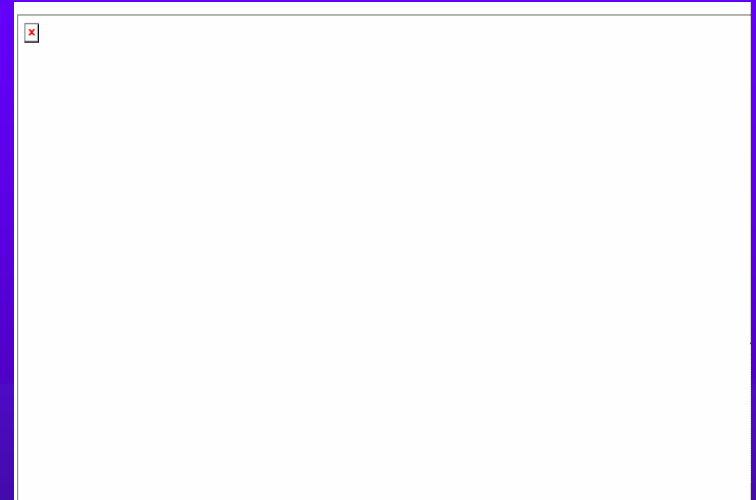
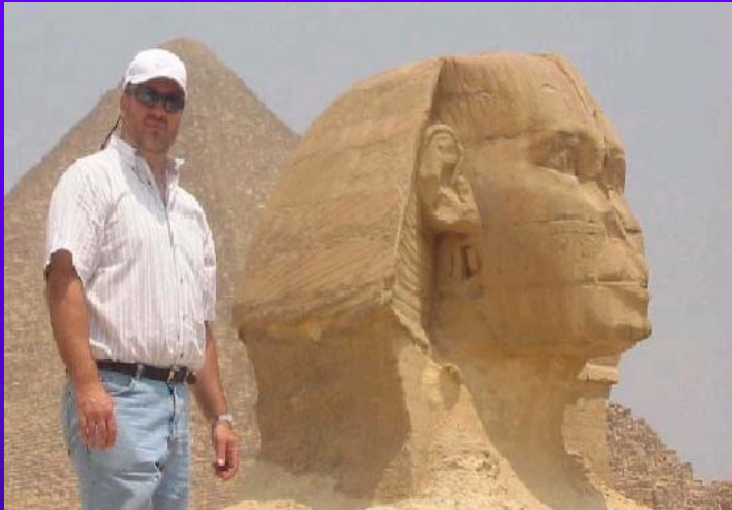
## ◆ Analysis Areas

- Email
- Temp Files
- Recycle Bin
- Info File Fragments
- Recent Link Files
- Spool (printed) files
- Internet History (index.dat)
- Registry
- Unallocated Space- free space on the hard drive
- File Slack- free space between the end of the logical file and the end of physical file (cluster)
- RAM Slack- free space between the end of the logical file and the end of the containing sector
  - Sector- the smallest group that can be accessed on the disk. A group of disk sectors as assigned by the operating system are known as clusters.

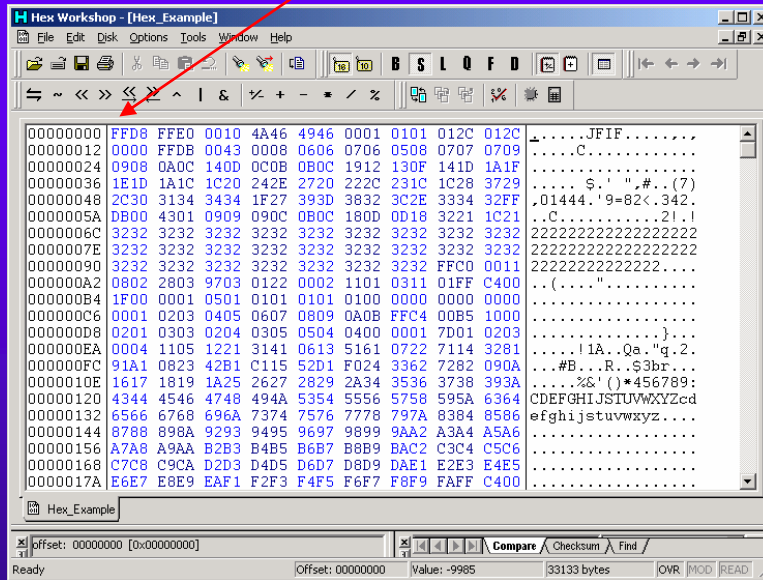




# What's the Difference?



# Here's the difference



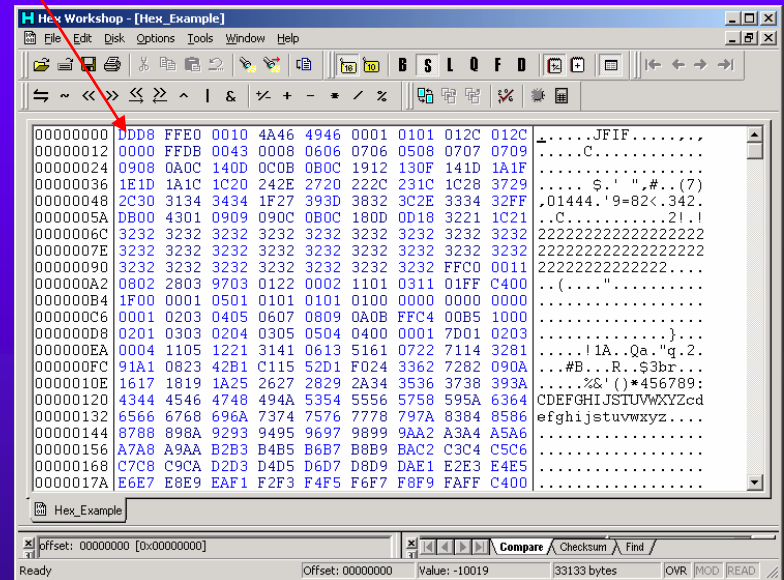
Hex Workshop - [Hex\_Example]

```
00000000 FFD8 FFED 0010 4A46 4946 0001 0101 012C 012C .....JFIF.....
00000012 0000 FFDB 0043 0008 0606 0706 0508 0707 0709 .....C.....
00000024 0908 0A0C 140D 0C0B 0B0C 1912 130F 141D 1A1F .....$.'",#..(7)
00000036 1E1D 1A1C 1C20 242E 2720 222C 231C 1C28 3729 .....01444.'9=82<.342.
00000048 2C30 3134 3434 1F27 393D 3832 3C2E 3334 32FF .....C.....21.!
0000005A DB00 4301 0909 090C 0B0C 180D 0D18 3221 1C21 .....C.....21.!
0000006C 3232 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
0000007E 3232 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
00000090 3232 3232 3232 3232 3232 3232 3232 3232 3232 2222222222222222...
000000A2 0802 2803 9703 0122 0002 1101 0311 01FF C400 ..(.....".....
000000B4 1F00 0001 0501 0101 0101 0100 0000 0000 0000 .....
000000C6 0001 0203 0405 0607 0809 0A0B FFC4 00B5 1000 .....
000000D8 0201 0303 0204 0305 0504 0400 0001 7D01 0203 .....}...
000000EA 0004 1105 1221 3141 0613 5161 0722 7114 3281 .....!1A..Qa."g.2.
000000FC 91A1 0823 42B1 C115 52D1 F024 3362 7282 090A .....#B...R..$3br...
0000010E 1617 1819 1A25 2627 2829 2A34 3536 3738 393A .....%&'()*456789:
00000120 4344 4546 4748 494A 5354 5556 5758 595A 6364 CDEFGHIJSTUVWXYZcd
00000132 6566 6768 696A 7374 7576 7778 797A 8384 8586 efg hijstuvwxyz....
00000144 8788 898A 9293 9495 9697 9899 9AA2 A3A4 A5A6 .....
00000156 A7A8 A9AA B2B3 B4B5 B6B7 B8B9 BAC2 C3C4 C5C6 .....
00000168 C7C8 C9CA D2D3 D4D5 D6D7 D8D9 DAE1 E2E3 E4E5 .....
0000017A E6E7 E8E9 EAF1 F2F3 F4F5 F6F7 F8F9 FAFF C400 .....
```

Hex\_Example

Offset: 00000000 [0x00000000] Compare Checksum Find /

Ready Offset: 00000000 Value: -9985 33133 bytes OVR MOD READ



Hex Workshop - [Hex\_Example]

```
00000000 DDD8 FFED 0010 4A46 4946 0001 0101 012C 012C .....JFIF.....
00000012 0000 FFDB 0043 0008 0606 0706 0508 0707 0709 .....C.....
00000024 0908 0A0C 140D 0C0B 0B0C 1912 130F 141D 1A1F .....$.'",#..(7)
00000036 1E1D 1A1C 1C20 242E 2720 222C 231C 1C28 3729 .....01444.'9=82<.342.
00000048 2C30 3134 3434 1F27 393D 3832 3C2E 3334 32FF .....C.....21.!
0000005A DB00 4301 0909 090C 0B0C 180D 0D18 3221 1C21 .....C.....21.!
0000006C 3232 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
0000007E 3232 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
00000090 3232 3232 3232 3232 3232 3232 3232 3232 3232 2222222222222222...
000000A2 0802 2803 9703 0122 0002 1101 0311 01FF C400 ..(.....".....
000000B4 1F00 0001 0501 0101 0101 0100 0000 0000 0000 .....
000000C6 0001 0203 0405 0607 0809 0A0B FFC4 00B5 1000 .....
000000D8 0201 0303 0204 0305 0504 0400 0001 7D01 0203 .....}...
000000EA 0004 1105 1221 3141 0613 5161 0722 7114 3281 .....!1A..Qa."g.2.
000000FC 91A1 0823 42B1 C115 52D1 F024 3362 7282 090A .....#B...R..$3br...
0000010E 1617 1819 1A25 2627 2829 2A34 3536 3738 393A .....%&'()*456789:
00000120 4344 4546 4748 494A 5354 5556 5758 595A 6364 CDEFGHIJSTUVWXYZcd
00000132 6566 6768 696A 7374 7576 7778 797A 8384 8586 efg hijstuvwxyz....
00000144 8788 898A 9293 9495 9697 9899 9AA2 A3A4 A5A6 .....
00000156 A7A8 A9AA B2B3 B4B5 B6B7 B8B9 BAC2 C3C4 C5C6 .....
00000168 C7C8 C9CA D2D3 D4D5 D6D7 D8D9 DAE1 E2E3 E4E5 .....
0000017A E6E7 E8E9 EAF1 F2F3 F4F5 F6F7 F8F9 FAFF C400 .....
```

Hex\_Example

Offset: 00000000 [0x00000000] Compare Checksum Find /

Ready Offset: 00000000 Value: -10019 33133 bytes OVR MOD READ



What Does It Take to Do Forensics?



# Hardware

- ◆ Become familiar with the inside of the computer
- ◆ Understand hard drives and their settings
- ◆ Motherboards
- ◆ Power connections
- ◆ Memory



# Knowledge of Operating Systems and Software

- ◆ Operating Systems
  - Microsoft Products
  - Linux RedHat
  - UNIX
- ◆ Software
  - Forensic Software
  - HTML
  - Microsoft Office
  - Quick View Plus
- ◆ "Jack of All Trades"



# Training

- ◆ New Technologies (NTI) in Gresham, Oregon
- ◆ Guidance Software (Encase)
- ◆ Access Data
- ◆ HTCIA Annual Conference
  - HTCIA 2002 October 1<sup>st</sup> - 3<sup>rd</sup> in Atlantic City, NJ



# Patience

- ◆ One needs the ability to be able to sit in front of the computer and analyze the data for what could be an extensive amount of time.
- ◆ "No such thing as point and click forensics."



# Contacts in the Industry

- ◆ HTCIA

- ◆ ListServes

- Computer Forensic Investigative Digest (CFID)

- [www.infobin.org](http://www.infobin.org)

- High Tech Crime Consortium (HTCC)

- [www.hightechcrimecops.org](http://www.hightechcrimecops.org)



# Forensic Case in the News



BUSINESS

## The Company of Spies

The FBI busts a small firm for funneling technology to China—but it wasn't about bombs

By MASSIMO CALABRESI

**N**UCLEAR WARHEADS. THAT'S WHAT comes to mind when the words China and espionage are put together. But a less geo-strategic although perhaps more pervasive form of Chinese spying returned to the headlines last week—one focused not on ideology but on gutsy entrepreneurship and pure capitalism. No nukes this time. Instead, the target was technology for an advanced consumer-phone system. Arrested in the incident were a trio of business partners, all Chinese immigrants, including two employed by New Jersey-based Lucent Technologies. They had dreamed of an American shortcut to their country's capitalist road. In an e-mail pitch to Beijing venture capitalists, one of the accused said their company would become "the Cisco of China."

It was Lucent, however, and not Cisco that suffered the alleged theft in a case emblematic of a fresh direction in spying. Private companies and individuals were behind more than half the incidents of industrial espionage in 1999, the most recent year for which statistics are available from the National Counterintelligence Center. Chinese commercial spies—not necessarily working for their government—have joined a throng of other agents targeting American know-how, including those from such ostensible U.S. allies as Japan, Israel, France and South Korea.

Two of the Lucent suspects left China to seek academic and monetary success in America, part of an influx of foreign-born scientists and engineers who helped propel the U.S. to R-and-D. dominance in the 1980s and '90s. Hai Lin, 30, got a Ph.D. from the New Jersey Institute for Technology in 1996, while his future colleague at Lucent, Kai Xu, 33, got a doctorate in 1995 from Rutgers. Both found work through a technology-employment firm that places talented technicians with



**INSIDE LUCENT**  
Kai Xu and Hai Lin were "distinguished members" of the red-logged firm's engineering staff

companies that need their expertise. For two years they worked as "distinguished members" of Lucent's staff, making six-figure salaries and settling into comfortable lives in suburban New Jersey. It is not clear when the two made contact with the third suspect, Yong-Qing Cheng, a vice president at the New Jersey-based IT company Village Networks. But according



**COME ON IN** China's President Jiang Zemin was given a tour of a research lab at Lucent's headquarters in 1997

to investigators, the combination of Lin and Xu's insider knowledge of Lucent and Cheng's salesmanship led to the development of a business plan: take the source code for the PathStar Server, build a company around it and market it in China. In July 2000, Cheng traveled to Beijing to meet with the Datang company, an octopus of a communications conglomerate officially owned by the government but, like most such firms, charting its own chaotic routes to riches. Cheng secured at least \$1.2 million from Datang for a joint venture dubbed DTNET. Not bad for a little company launched in his New Jersey home and now impressively called ComTriad Technologies Inc.

But Lucent grew suspicious of Lin and Xu's activities and last February contacted the FBI and the U.S. Attorney's office in Newark, N.J., which began tracking the Internet exchanges of the two scientists. Without signs of independent product development at ComTriad, investigators nevertheless found e-mails allegedly showing the partners' listing "intellectual assets" identical to those of PathStar and discussing product presentations "based on PathStar." And unfortunately for Lucent, the e-mails show that by the time the feds were on the case, the PathStar source code was in Datang's hands. It will be harder to recover than a U.S. spy plane in Hainan—if not impossible. Investigators say there is no indication of any criminal act by Datang and the Chinese government, nor any indication that Beijing and its conglomerate knew their joint-venture partner ComTriad was acting illegally.

Like many American companies, Lucent has invested millions in (and signed lucrative contracts with) Chinese companies. The incident is unlikely to dampen the company's ardor—or that of any other U.S. firm—for the promise of China capitalism. But the bottom line isn't likely to be profitable for three Chinese partners in America. The men are to be charged with wire fraud. Each faces five years in jail and \$250,000 in fines. Cheng is a naturalized American; Lin and Xu were only months away from their green cards. Hoping to be the Cisco of China, they may have forfeited the right to make it in America.

—With reporting by  
Desa Philadelphia/New York



"That's All Folks!"

[mbarba@computer-forensic.com](mailto:mbarba@computer-forensic.com)

[www.computer-forensic.com/presentation](http://www.computer-forensic.com/presentation)