

- Cyber criminals are wreaking havoc on computer systems and are capturing front-page headlines in the bargain
- Fortunately, the computer security field is also progressing at a brisk rate.
- In particular, the field of computer forensics brings new ways of preserving and analyzing evidence related to cyber crime
- The numbers are chilling. According to a recent industry survey, 94% of the survey respondents detected cyber-attacks on their companies, and 617 organizations reported \$609,923,384 in financial losses

- So what's going on- It doesn't take a computer engineer or computer scientist to learn hacking fundamentals.
- After spending a few nights on the Internet, high school students discover they can master hacking fundamentals by simply downloading software
- Colleges have finally started to offer courses and concentrations in computer security and forensics.

- Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information.
- The fascinating part of the science is that the computer evidence is often transparently created by the computer's operating system without the knowledge of the computer operator.
- **The information may actually be hidden from view. To find it, special forensic software tools and techniques are required.**

- Most law enforcement agencies, especially those in large cities, are understaffed when it comes to having trained computer forensics experts.
- Industry, on the other hand, has been taking computer forensics.
- The biggest issue surrounding the computer forensics is a shortage of technologists who have the working knowledge of computer forensic seriously for several years

- There's an old saying, "If you wait long enough, it's bound to change." The same can be said for computer forensics training.
- Not only will more techies be concentrating on computer forensics, but also attorneys and judges will be taking courses in the subject.
- Learning forensics basics will help attorneys especially to determine the kinds of evidence that can be found by probing a computer's operating system and what techniques can be used to legally obtain it.
- On the academic front, full-fledged degree tracks in computer forensics are being developed. Certification programs already exist.

- **Where are the jobs? Government agencies, such as the Department of Defence, FBI, CIA, NSA, and U.S. Postal Service need computer forensics specialists.**
- **State and local law enforcement departments are also hiring computer forensics specialists.**
- **On the corporate front, all companies (especially large and mid-size ones with a Web presence) will have serious computer forensics needs.**
- **Job titles differ, but, typically, these positions are advertised as junior computer forensics analysts for entry-level jobs and senior computer forensics analysts if you have a few years of experience in the field.**