# SNS COLLEGE OF TECHNOLOGY

**(Autonomous)**
COIMBATORE – 35

**DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)**

**Third Year Computer Science and Engineering, 5th Semester**

**UNIT II - CYBER FORESENICS**

**Topic Name : Historical background of Cyber forensics**

Historical Background of Digital Forensics

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 - 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

It is difficult to pinpoint when computer forensics history began. Most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state, and federal level. Private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.

The computer forensic field continues to grow on a daily basis. More and more large forensic firms, boutique firms, and private investigators are gaining knowledge and experience in the field. Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.