AGENDA

Reconstructing Past event Networks

Reconstructing past events

- *Recovered data must be analysed and the file must reconstructed using advanced search programs specifically developed for this work*
- *These techniques were recently used to recover data from computers that indicated large forgery and personal and business identities being stolen without knowledge of victims*
- *In a murder case the murders computer address book was recovered and now analysed to see if he is serial killer*
- *A stalker who had restricted page info on his victim which was recovered from suspects computer*

How to Become a digital detective

- Once data is recovered you need make sure it is admissible
- **Some tips**
- ***If you need help , get help***
- ***Convert digital evidence***

How to Become a digital detective

- ***Put the evidence in a usable format***
- **Usable File formats**
- Ex: we will not able to open old word file if we are using WordPerfect 5.1
- **Unusable file formats**
- .Txt file fully corrupted

Network Forensics

- A high profile computer system was compromised and case was in investigation
  - A network security system has been retaining all network packet info for past six months
  - Advanced visual tools were applied tens of millions of network events
  - Along with visual tools and info produced from on site investigation were used to identify suspect communication
  - Pattern analysis
  - Other abnormalities were identified by visually mining thru forensic data

Network Forensics- Data Visualizer

- Components
  - Network forensic data & database
  - Visual query interface
  - Network forensic data visualizers

Destruction of email

- Courts treat emails as formal records
- Companies email is discoverable in litigation
- Oliver north white house case
- Any attempt to destroy the official email is punishable under law

Standards

- Standard operating procedure (SOP) are documented that must be supported by court and other agencies.
- Chain of custody need to be maintained

Principles against damage of computer evidence

- International principles developed by IOCE
  - Consistency with all legal systems
  - Allowance for the use of a common language
  - Durability
  - Ability to cross international boundaries
  - Ability to instil confidence in the integrity of evidence
  - Applicability to all forensic evidence

Documenting the intrusion on destruction of data

- Incident reporting and contact forms
- Important components of the forms
  - Contact information for person(s) discovering problem
  - Target systems and/or networks
    - Know all about the systems under attack including OS versions, IP addresses and so on
- Purpose of system under attack
  - Know which systems are used for

Some kind of ranking for the importance of the system