COE589: Digital Forensics

Overview and Logistics

Dr. Ahmad Almulhem
KFUPM – Spring 2013 (T122)
Digital Forensics

• **Forensic Science:** Applying science for the purpose of law
  – solve crimes
  – dealing with weapons, blood, fingerprints,

• **Digital Forensics:** Forensics in the digital world
  – obtaining and analyzing digital information
  – bringing evidence in civil, criminal, or administrative cases

• originated as **computer forensics (80’s)**
  – all devices capable of storing digital data
Digital Forensics

Forensics Science

Digital Forensics

computer forensics
mobile forensics
network forensics
Why Digital Forensics is important?

• **crime** scenes increasingly involve digital devices
  – traditionally deal with physical evidences: weapon, blood, fingerprints
  – cybercrimes: Fraud, child pornography,
• not just crimes; internal **investigations** as well
Digital Evidences everywhere

- DF enabler is digital world of communications and activities
- Digital traces are everywhere (very hard to destroy!)
  - computers, PDAs, cellular phones, videogame consoles, digital cameras, copy machines, printers, etc...
Digital World

- 93% of information created, modified and consumed entirely in digital form (UC-Berkeley 2001)
  - spreadsheet,
  - databases
- social networking
  - forums
  - twitter
  - facebook
Computer/Network Attacks

• Malware
  – viruses, Trojans, etc.
• Industrial attacks (Aramco)
• Hacktivism
  – hacking for political reasons
• Mobile malware
• Spam
• ....
Computer Crimes are Expensive

UK cyber crime costs £27bn a year - government report

Cyber crime costs the UK economy £27bn a year, the government has said.

The figures, published for the first time, are a mid-range estimate and the real cost could be much higher.

They are made up of £21bn of costs to businesses, £2.2bn to government and £3.1bn to citizens.

Security minister Baroness Neville-Jones said the
Digital Forensics Saves Life

• In 2004, Bobbie Jo Stinnett was murdered and her unborn baby “kidnapped”
• Police examined her computer and traced an IP address to Lisa Montgomery
• Montgomery had corresponded with Stinnett over the Internet
Digital Forensics Multi-disciplinary

Computer Technology

Investigative Techniques

Law

Science & Engineering

Art & Expertise

COE589 - Ahmad Almulhem
Why Should You take this course?

• Learn about Digital Forensics
  – hot area

• Learn to conduct research in Digital Forensics
  – Pick a topic for your MS/PhD thesis

• Learn to conduct research in general
  – effective paper reading
  – technical paper writing
COE589: Digital Forensics