COE589: Digital Forensics

Research in Digital Forensics

Dr. Ahmad Almulhem
KFUPM - Spring 2013 (T122)
Outline

• What is (not) Research?
• Research Agenda for Digital Forensics
• Future Research in Digital Forensics
• Re-Visit to Course Syllabus
Research

• Research is creative work undertaken systematically to increase knowledge of society (or human in general)
  – establish or confirm facts
  – reaffirm the results of previous work
  – solve new or existing problems
  – expansion on past work in the field
  – ....
Research is NOT ...

• Research is NOT Search
  – Google will not make you a good researcher!

• Research is not about gathering information
  – Gathering information from books, magazines, and Internet is not research
  • Does not contribute to new knowledge

• True research requires comprehension and synthesis
Research Steps

1. Identification of research problem
2. Literature review
   – identifies flaws or holes in previous research
3. Determine specific research questions
4. Data collection/build a prototype
5. Analyzing and interpreting the data
6. Reporting and evaluating research

[Hourglass model diagram with 'repeat' text]
Research in Digital Forensics

• Digital forensics is largely practitioner-driven field
  – Advances are reactions to a specific incidents or needs
  – a “bottom-up” development
• Other fields contributed independently into DF
• Can be hard to identify research taxonomy
  – specific topics
  – concrete problems
Research in Digital Forensics

• "Digital Forensics: Defining a research agenda", K. Nance et al, 2009

• Group of DF researchers, educators, practitioners met to define a DF research agenda
  – identify research areas
  – explore categories, subcategories,
  – provide concrete examples within individual categories
  – tool: brainstorming, free-format discussion
DF Research Agenda

- Findings: six research categories:
1. Evidence Modeling

Goal: simplify the investigation process for investigators

• Modeling the investigative process
• Case modeling for particular types of crimes (e.g. embezzlement, child pornography, etc.)
  – data collection: identify relevant data
  – data organization: better processing, analysis, presentation
  – re-use of past cases
2. Network Forensics

- Forensics on end-points (workstations, servers) is somewhat clear
- How about non-end points
  - switches, routers, ..etc
- How about non-traditional network device
  - printers, copiers, home automation, ... etc
- Automated data collection triggered by IDS
3. Data Volume

- Typical investigation can involve massive volumes of data
  - increasing storage capacities
  - multiple storage
- Parallel processing (high performance computing)
  - imaging
  - carving
  - history timeline
  - ...
4. Live Acquisition

• Forensics of a powered-down system is generally understood and accepted
  – storage media
• Forensics for a live system is important and challenging
  – network connections, encryption keys, process list, .. etc.
• Research topics:
  – Analysis of RAM dumps
  – Analysis of physical RAM with interrupting execution (Virtualization)
  – Analysis of physical RAM without interrupting execution (??)
  – How about legal issues? How accurate is the analysis?
5. Media Types

• Computer forensics evolved into Digital Forensics
  – devices such as phones, digital cameras, and game consoles

• Cell phones have no standard interface, either at the hardware or software levels
  – analysis process is unique for each device model
6. Control Systems

• Forensics for process control systems (SCADA Systems)
  – computer systems that monitor and control industrial, infrastructure, or facility-based processes

• Most of them are built to control processes, not to track them

• Largely un-explored area of research!
DF Research Future

• "Digital forensics research: The next 10 years", S. Garfinkel, Digital Investigation 2010

• Jump to the authors slides
Course Objective Review

• Re-Visiting our course syllabus: