Investigations

CIS8630 Business Computer Forensics and Incident Response
Richard Baskerville

Georgia State University

With thanks to Collin Armstrong, Curtin Business School

Investigation Objectives

Investigation Yields Evidence That Is Hard to Find

The investigators are going to have to find the evidence. They are going to have to investigate. They have to find out the facts, and then be able to demonstrate those facts and findings to others and be able to justify their findings in an adversarial environment.

- Collin Armstrong

Basics of Investigation

“It is elementary, my dear Watson”

- Dr. Joseph Bell
  - 19th C forensics surgeon
  - Inspiration for the Holmes character
- Sherlock Holmes to Dr. Watson, “A detective needs three things for success,”
  - The Power of Observation
  - The Power of Deduction
  - A Wide Range of Exact Knowledge
- Forensic practitioner need sound knowledge and experience of:
  - The Law
  - IT
  - How to conduct an investigation

Reasons for Investigating

Prevention and Responsibility

- Future prevention by knowing what & how “something” happened – able to combat and prevent or lessen impacts of future occurrences.
- Victims have a responsibility to community to permit gathering & analysis of evidence which may lead to prosecution, greater public awareness, and other potential victims to prepare defenses aimed at preventing or lessening impacts of future occurrences.
Investigation Techniques

Differing Needs, Constraints, and Approaches

- **Pro-Active versus Reactive**
- **Law Enforcement versus Private - Corporate**

Investigation Organizing Principles

- Ad Hoc
- Needle in the hay stack
- Rule-of-thumb method
- Red handed
- Serendipitous
- Haphazard
- Gut instinct
- Politically or religiously inspired
- Scientific method

Investigations

CIS8630 Business Computer Forensics and Incident Response
Richard Baskerville

With thanks to Collin Armstrong, Curtin Business School

Sample Investigation Plan

Colin Armstrong, Curtin University

- **Determine the Objectives**
  - Ascertain the facts regarding an allegation that improper conduct has occurred and that they have been perpetrated by a particular named individual.

- **Define the Task**
  - Visit location of alleged incident
  - Obtain true and exact copy of Computer data. Record all relevant information at site

- **Gather Evidence**
  - Tag and bag all evidence gathered.
  - Collect evidence
  - Photograph site
  - Confirm management consent, approval, encouragement for commencing investigation.
  - Comply with the rules of evidence
  - Protect innocent parties and vital evidence
  - Watch for patterns of behaviour and possible motives that may assist in determining potential suspects, and look for an appropriate response to prevent similar occurrences
  - Be aware of the extent of the losses incurred and possible means of recovery.

- **Determine the Methods & Tools**
  - Time frame for Investigation
  - Determine who are the people of interest
  - Interview people of interest

- **Is There a Company Policy on This Matter?**
  - If there is a company policy on this matter is it available to all staff?
  - Is the policy enforced?
  - Is the policy enforced uniformly?
  - Are staff aware of company policies on acceptable use?