Intro to Digital Forensics

Introduction

Image Capture

Microsoft Filesystems

Linux Filesystems

Evidence Analysis

Live Forensics

Network Data Capture

Network Capture Analysis

Data Forensics

Investigation Planning and Process

Network Device Forensics

Digital Forensics

Background

ISACA Digital Forensics Overview Video

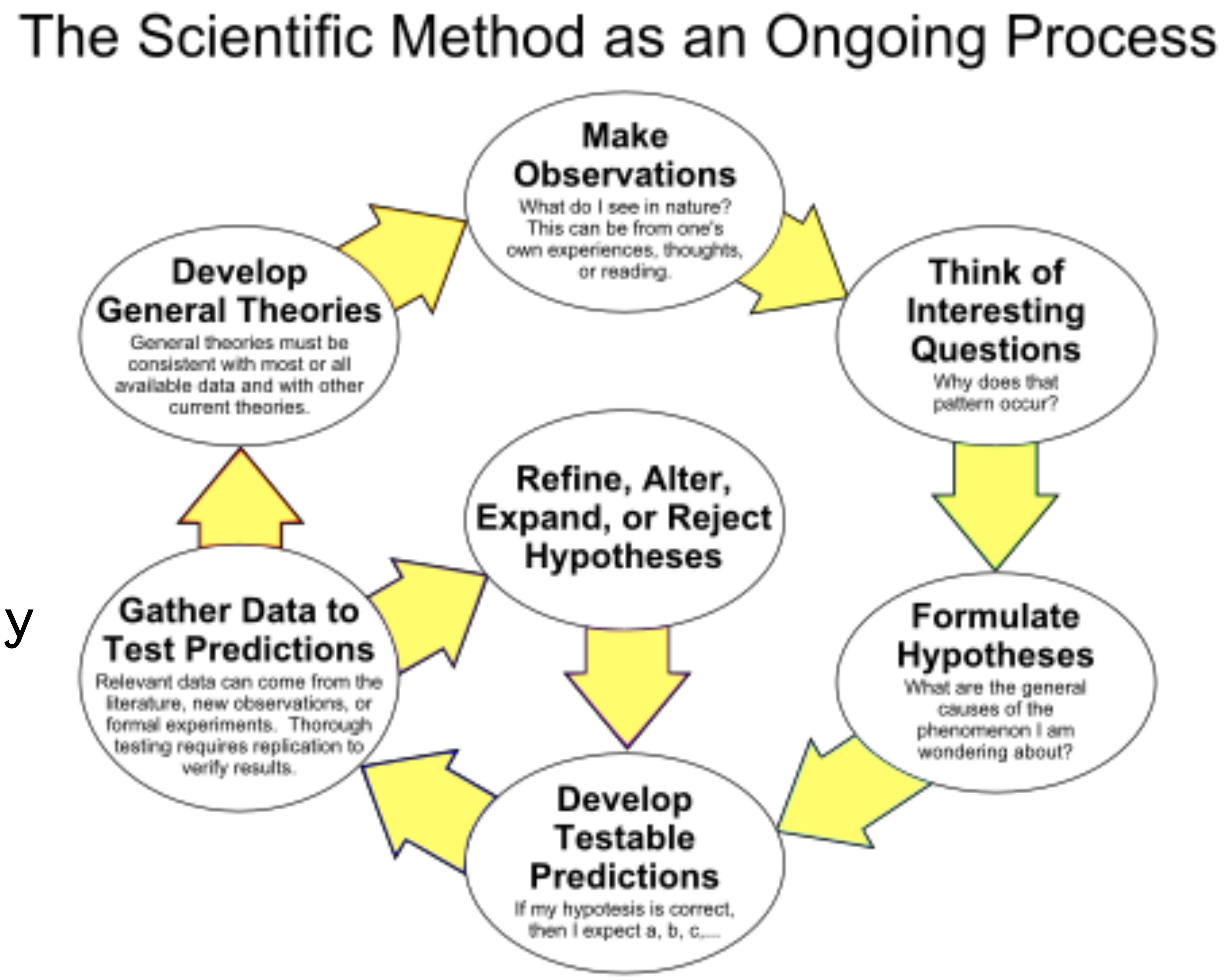
- Computer proliferation in the second half of the 1970s led to growth in the relevance of stored digital data to criminal activity
- This led to the first USA state law against unauthorized modification or deletion of data on a computer system in 1978 in Florida, and the FBI creating the Computer Analysis and Response Team (CART) in 1984
- Canada was the first nation to create federal laws covering computer offences in 1983, with the USA, Australia and Britain following suit in 1986, 1989 and 1990, respectively
- Modern laws cover not only what kinds of information can be used in legal matters and how, but also govern what may be collected and the processes for doing that collection (e.g. warrants, wiretaps, seized equipment, cellular/wifi interception, etc.)

What is Digital Forensics

- Examination of the recent past of digital entities using a process to credibly identify what has happened, theorize how it happened, and identify the actors involved in what happened when possible
- The scientific method is used to validate theories proposed
- Drawing conclusions about the significance of the discovered information, and determining what if anything to do with that information, are not forensic activities
- Digital forensics encompasses computer, network, memory or live, and data forensics, all of which are a subset of the considerably broader science of forensics

Scientific Method

- Provides an iterative method to reliably describe why phenomena occur
- Used in forensics to test theories proposed as explanations for observed data
- There are often many possible reasons why something may be observed, it is important to refine the possibilities into probable causes



The Scientific Method as an Ongoing Process

Make Observations
What do I see in nature? This can be from one's own experiences, thoughts, or reading.

Think of Interesting Questions
Why does that pattern occur?

Formulate Hypotheses
What are the general causes of the phenomenon I am wondering about?

Develop Testable Predictions
If my hypotesis is correct, then I expect a, b, c,...

Gather Data to Test Predictions
Relevant data can come from the literature, new observations, or formal experiments. Thorough testing requires replication to verify results.

Refine, Alter, Expand, or Reject Hypotheses

Develop General Theories
General theories must be consistent with most or all available data and with other current theories.

https://en.wikipedia.org/wiki/Scientific_method

Forensic Principles

- Mandate - fact-finding vs. conclusion drawing
- Non-contamination - required for reproducibility which is required for credibility
- Admissibility - facts are not necessarily considered in decision making, especially in legal proceedings
- Scope - too much data can lead to facts which are not specific, or can only be partially presented/used
- Confidentiality - affects access to evidence, dissemination of results

Uses of Digital Forensics

- Digital forensics provides a description of, and explanation for, digital phenomena
- These descriptions and explanations are useful in many activities, including these examples:
    - Criminal investigation/prosecution/defense
    - Civil litigation support
    - Corporate policy enforcement/investigation
    - Corporate liability mitigation
    - Black hat and white hat research
    - Administration of computers and networks

Forensic Process

SkillSet Forensic Investigation Process Video

- Identification of items which may contain relevant data (e.g. internal or external storage devices or services) or demonstrate valuable facts (e.g. destroyed CPU) and who has custody of them or their location
- Preservation of the evidence by controlling access to the devices, location, or personnel involved and documenting all of these
- Collection of the evidence which may involve seizing devices, taking over accounts, or making copies of data in various forms
- Analysis of the evidence leads to statements of fact and theories regarding those facts; analysis is supposed to discover objective facts but is often done in an attempt to prove or disprove a pre-determined explanation of the situation
- Reporting the evidence in a form useful for its intended purpose (evidence for use in court, records supporting corporate or HR actions, information about a situation used to aid in creating and testing defenses against that situation), reports from forensic software are not enough in most cases

Who does it

- Digital forensics activity is most effective when done by trained specialists, but most often is done by whoever is available
- Police and security agencies are the investigators or investigation supervisors when the investigation is related to criminal activity
- Private contractors and consultancy firms are involved when the investigation is related to civil legal matters or corporate liability matters
- Internal and outsourced IT personnel do forensic work in support of corporate operations, including human resources related investigations
- Administrative and security staff do forensic work in support of securing and effectively managing computer systems and networks

Authorization

- It is very important that whoever is doing the work is authorized to perform those activities and access the forensic data
- Lack of such authority can invalidate the evidence or investigation as well as conclusions drawn from them
- It can also create liability for the investigator and whoever they are acting on behalf of
- It can create unintended problems by running afoul of protections on the evidence (e.g. seeing details of transactions protected by confidentiality agreements unrelated to the intended investigations)

Evidence Gathering

- Modern laws provide law enforcement with tools for use in gathering evidence (e.g. warrants, seizure)
- Modern laws also provide expectation of privacy protections for citizens, and rules of liability and conduct for corporations
- Disclaimers (e.g. warning banners at login, employment contracts, non-disclosure agreements, etc.) can help provide authorization for investigation so that evidence is admissible and investigative activities are not subject to prosecution or civil suit
- For the same reasons, it is important to always maintain professional conduct when investigating to build and preserve your reputation and credibility
- Evidence gathered for use in court has strict rules governing how you collect, handle, and preserve or transfer it; these rules vary from jurisdiction to jurisdiction even within a country, state, or province
- Evidence can be inculpatory (incriminating) or exculpatory or irrelevant

Reasonable expectation of privacy in Canada - article in Canadian Lawyer magazine

Types of Digital Forensics

- Computer
- Network
- Mobile Device
- Memory (aka Live Acquisition)
- Data (images, audio, video, structured data)

Computer Forensics

- Computer forensics uses the physical components of the computer as evidence
- The investigation normally focuses on secondary storage (disks, memory sticks and cards, backups), and the results may lead to data or disaster recovery activities
- If the incident involves physical tampering, modification, or damage, then other components may be part of the evidence, including things related to gaining physical access to the computer such as physical or electronic lock or interlock mechanisms, or power or connectivity provision devices

Network Forensics

- Investigates network events and data
- Tries to identify who did what, when they did it, and to what or whom it was done
- Investigation may include determining the incursion vector, as well as what was done once access what obtained
- Can be done live, but is usually done by examining logs and traffic capture files

Mobile Device Forensics

- A very new area which ranges from simple device software and settings examinations to filesystem investigation
- The strong relationship of mobile devices to the network means this activity can rely on correlating evidence on the device with network forensics
- It is otherwise just a specialized version of computer forensics, complicated by the non-removable nature of their storage devices, the volatile nature of the storage (on-chip controllers constantly modify things, even if you don't try to write to the device), and the added complexity of filesystem formats designed for limited write-count NAND devices

Memory Forensics

- Forensics is traditionally a reaction to an event or in response to a request for support or refutation of an interpretation of a situation
- Memory-based forensics, or live forensics is a proactive activity designed to audit current activity or events
- Helpful to catch bad actors red-handed, and to aid in developing system and network management and security
- May also be required to access data secured by session keys or login credentials

Data Forensics

- For multimedia data, this is the process of identifying changes made to a graphic image (e.g. a photo or original digital work), video file or files, or audio file
- It involves working with chain of custody and detailed knowledge of the expected data and metadata of the files
- For more complex data such as documents and datastores, the evidence to examine may include logs from the software and systems which had access to the stored data

Potential Impacts of Forensic Evidence

- Forensic evidence can be a valuable part of the legal process
- It can be used simply as objective information, but is usually used to support pre-determined positions in adversarial proceedings whether of a legal nature or not
- As a digital forensics investigator, your role is to produce truth as much as you are able, and leave the conclusions to those using the information you provide, otherwise you are tainting the process and undermining the credibility of your results

Forensic Science: Last Week Tonight with John Oliver Video

Standardization In Forensics

- ISO 27000 is a broad set of information systems security standards, including digital forensics
- SWGDE - Scientific Working Group on Digital Evidence (swgde.org) is a USA-based group of law enforcement professionals who meet and publish regularly in an effort to promote and advance digital forensics
- ENFSI - European Network Of Forensic Science Institutes (enfsi.eu) is recognized as the monopoly organization in the field of forensic science by the European Commission
- Many governmental and non-governmental organizations have their own standards for one or more aspects of digital forensic activities

Organizations Advancing Forensic Practices

- Government law enforcement and intel agencies
- Collaborations between companies
- Companies and non-profits doing business in the sector

Background Reading

- The course github site has links to several videos (about a half hour total) from SkillSet with overviews of computer investigations, as well as background reading about Canadian legal issues surrounding digital evidence acquisition and use in court