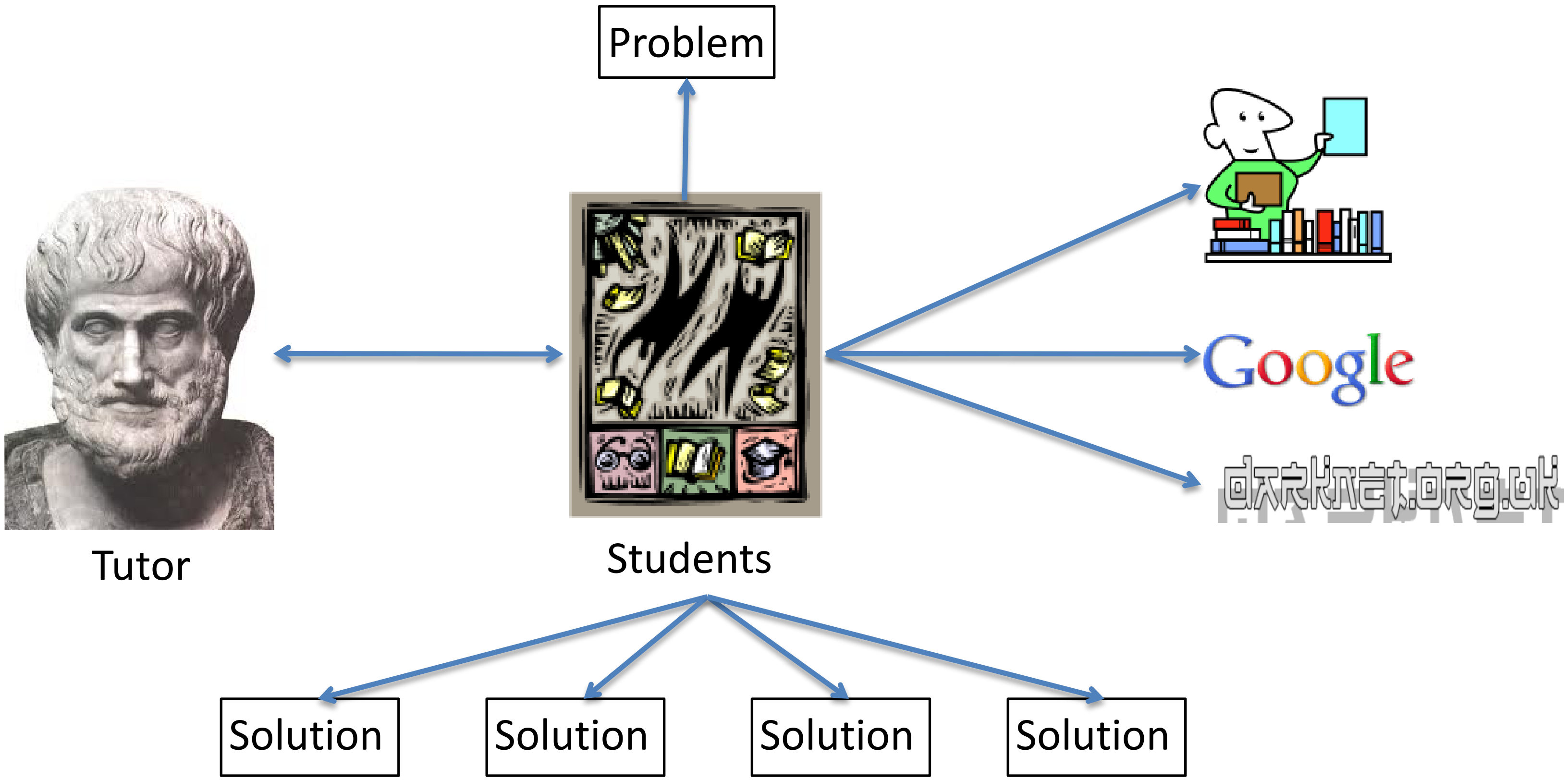
Individualising Problem-Based Learning

Michael Jones

Bournemouth University

Problem-Based Learning



Problem

Tutor

Students

Solution

Solution

Solution

Solution

Digital Forensics

- Emphasis on analysis and interpretation
- Variety of data sources
  - File systems (directory structures)
  - Browser, email, log data
  - Etc.
- Large number of (potential) tools
  - primitive
  - ‘professional’

The Scenario

- A gang has commissioned the production of plates to be used in creating counterfeit bank notes
- Police have captured an SD card hidden in a camera
- Police need to know:
  - Where and when the plates are being exchanged
  - Who is involved

Individual Learning Experience

- Same:
  - Scenario
  - Learning experience
- Different:
  - Data
  - Targets
  - File structure

Step 1: Data Generation

- The Forensic Case generator (FCG) creates the following for each image (student):
  - Contact information (names, mobile numbers)
  - GPS locations of the exchanges
  - Times and dates of the exchanges
  - Password
  - Bank account details
- How:
  - Using regular expressions (e.g., 07[0-9]{9})
  - Source data (e.g., file of first names, GPS of well-known locations)

Step 2: File Manipulation

- Data encoded and embedded in target files:
  - Metadata in PDF or HTML files; EXIF data in JPEGs
  - Hidden in text files, encrypted files, SQLite files
  - In a fragmented (tiled) image
  - In sound files
  - Etc.
- Encodings available include:
  - Base 64
  - Nato

Step 3: Population

- File system created
  - (currently FAT32, others imminent)
- Populated with a directory structure containing:
  - Directories
  - Manipulated files
  - Other files
  - Renaming and placing policies available

Step 4: Rendition

- File structure copied to target device or file system
- Files/directories deleted
  - Deletion policy available

What the students have to do

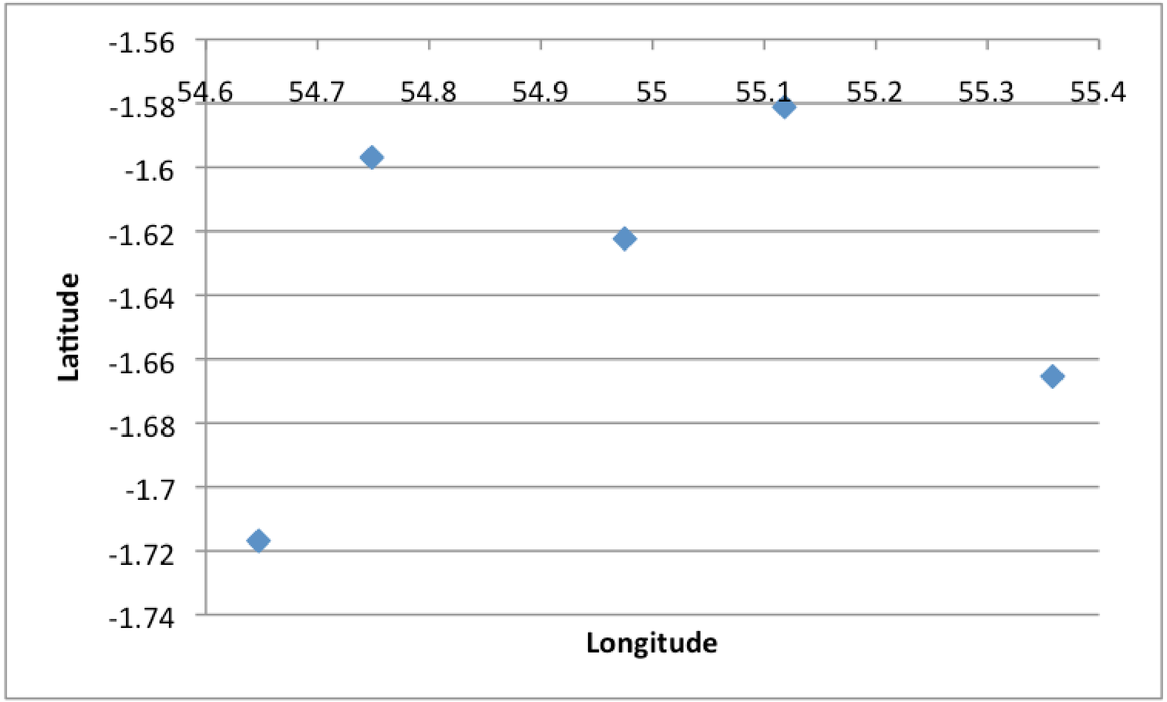
- Find the hidden information
- Identify all the files
- Write up to a standard suitable for use in a case
- Meta-learning
  - Seeing data as it is
  - Assessing the quality of data

Example GPS Data

- Landmark selected
- Points generated
- Students need to find the points and interpret data

Point 001	55	7	5.68	N	1	34	52.07	W
Point 002	54	38	50.40	N	1	43	0.63	W
Point 003	54	44	55.54	N	1	35	48.88	W
Point 004	55	21	30.12	N	1	39	55.47	W

Intersection



Intersection point: St James's Park, Newcastle

Question: intersection point is not in the data. Is it allowable as evidence?

Example Password Data

- Password: moeszyslak
- Nato encoding with partitioning:
  - ***M***ike ***O***scar ***E***cho
  - ***S***ierra ***Z***ulu ***Y***ankee ***S***ierra
  - ***L***ima ***A***lpha ***K***ilo
- Encoding:
  - One part rendered as a PNG image and then ‘tiled’
  - Another part dubbed over a WAV file
  - Final part encoded in base64 then embedded in a file

The Benefits

- Students can use any tools
- Students can help each other
- Problem segmentation or delay ineffective
- Images are easily scalable
- It is possible to organically influence problem-solving techniques
- Fun for students and staff...

Student Experience

- Forensic Computing & Security started in 2009
- First version of software used in first cohort
- Students report that fully analysing the image takes a long time
  - But no complaints – verbal or otherwise
  - Lots of positive comments

The Framework

- Goal: flexible data generator with minimum number of constraints
- Organised as a workflow
- Flexible in terms of:
    - Applications inclusion and sequencing
    - Data generation, selection of targets, embedding
    - Policies: naming, placing, deleting, etc.
    - Configuration via spreadsheet

Next…

- Use in other contexts
  - So far…
    - collaboration with ‘real’ CSI simulation
    - Used in Erasmus Intensive Programme
- More applications
  - E.g., logs, SQLITE files
  - E.g., GPS timeline
- Open source?

Thank you.

Questions?