Digital forensic analysis of the Raspberry Pi

Dhruv M. Saxena, Delhi Technological University,
dhruvmsaxena@gmail.com

Supervisor: Dr. Sarah Morris, Centre for Forensic Computing

Cranfield UNIVERSITY
Centre for Forensic Computing

Forensic Computing

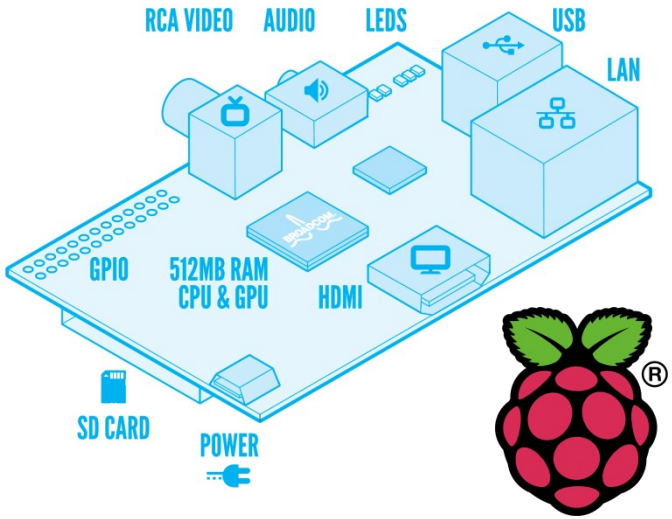
- Forensic Computing is the application of forensic science to computer base material. It involves:
  - Identifying the evidence
  - Determining how to preserve the evidence
  - Extracting, processing and interpreting the evidence
  - Ensuring that the evidence is acceptable in a court of law.
  - Documentation and Reporting
- Specialized Software.
- Knowledge about Law
- Dissecting computer system or network.
  - Retrieving deleted files
  - Tracing files
  - And MUCH MORE

Cranfield UNIVERSITY
Centre for Forensic Computing

Raspberry Pi

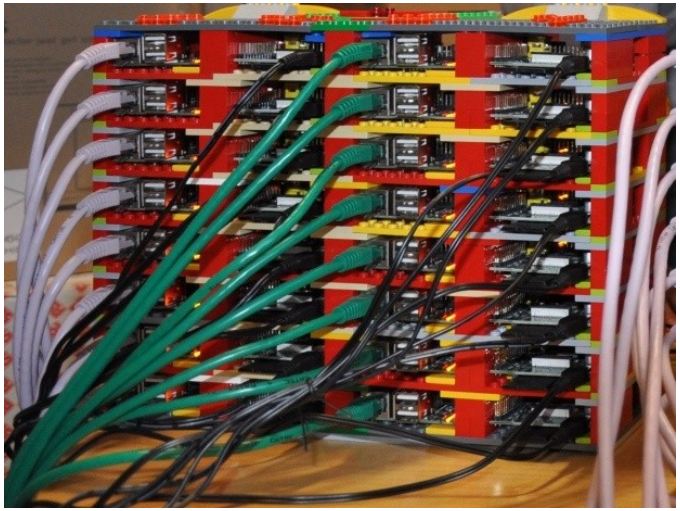
- Credit-card sized single board computer
- 700 MHz ARM11 processor
- 512 MB RAM
- HDMI, USB 2.0, Ethernet, Audio/Video ports
- GPIO pins

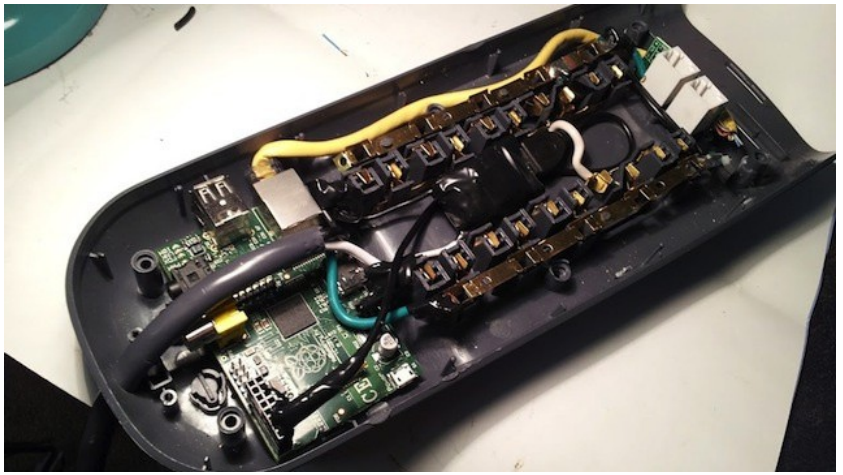
- Launched in February 2012 by the Raspberry Pi Foundation.



Why Pi?

- Price – £28 (Model B), £20 (Model A)
- Form factor – 85.60 mm × 53.98 mm
- Versatile – ports, pins, boards
- Linux based – multiple distributions, open-source



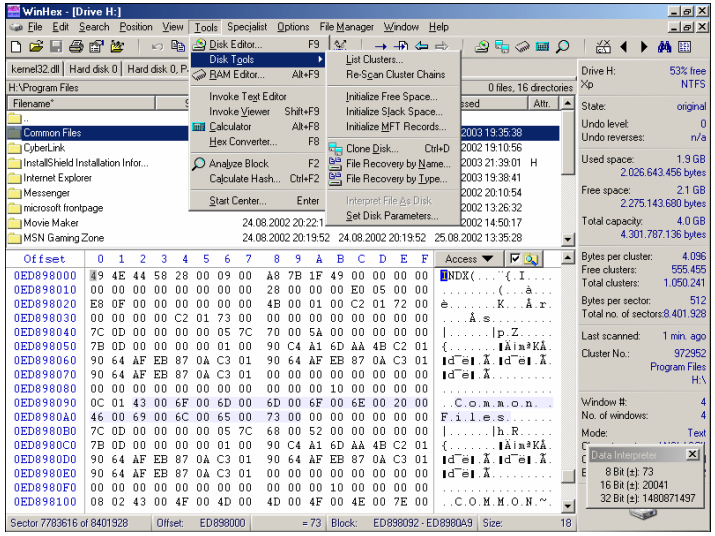


Getting Started with Digital Forensics

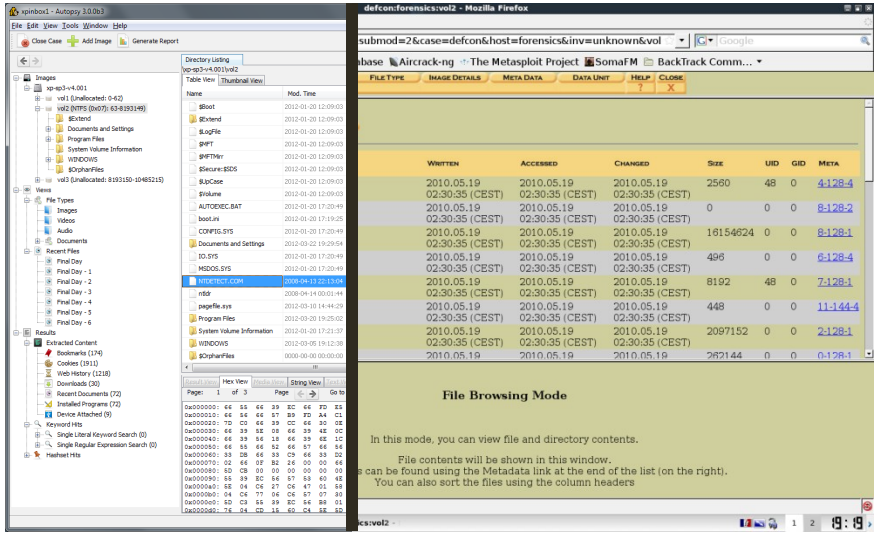
- Reading
  - ACPO Guidelines
  - Search and Seizure
- Test Case – Money Fraud
  - Used WinHex
  - Analysis of image(s)
  - Documentation
- Literature Review – for journal paper
- Python scripts
  - To compare images – baseline vs. experiment
  - To generate a HTML report
    - Of the comparison results
    - Of the system specs.
- Other Software
  - Autopsy for Windows/Linux
  - The Sleuth Kit
  - EnCase

Getting Started with Digital Forensics

- **Software**



WinHex

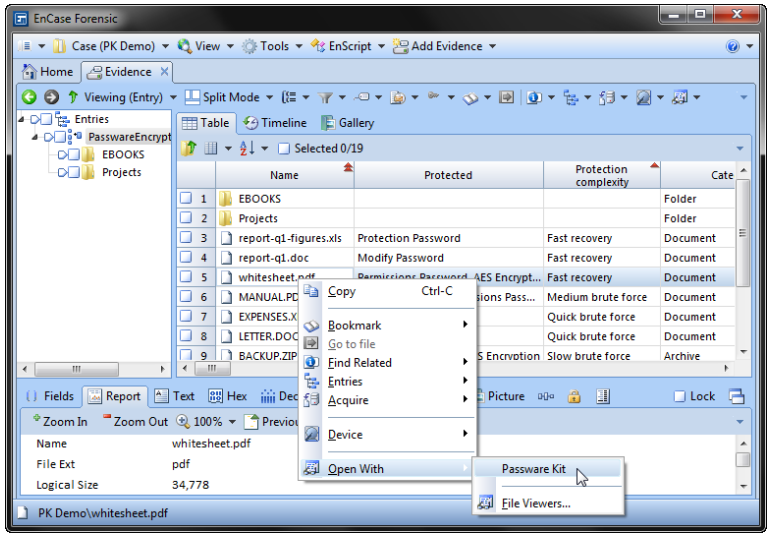


Autopsy for Windows/Linux
(based on The Sleuth Kit)

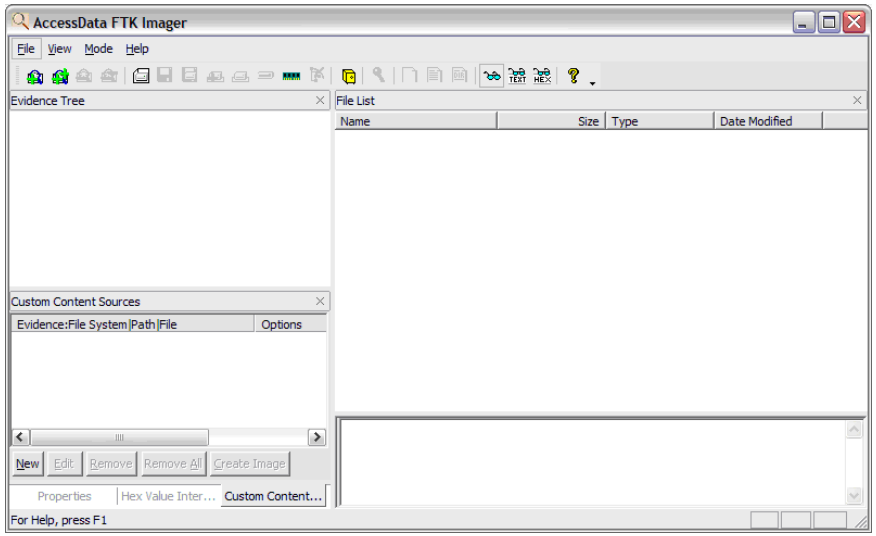
Cranfield UNIVERSITY
Centre for Forensic Computing

Getting Started with Digital Forensics

- **Software (contd.)**



EnCase



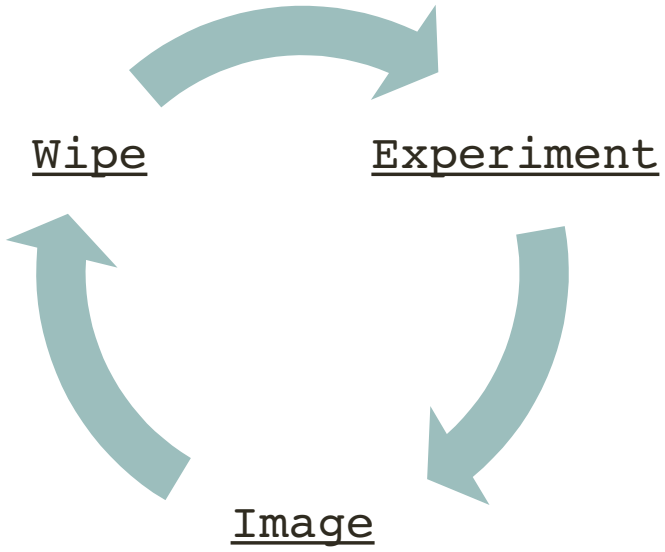
AccessData FTK Imager

Cranfield UNIVERSITY
Centre for Forensic Computing

Preliminary Research

- Raspbian emulation on QEMU
  - Look through the file system for places of interest
  - Imitate general user activity and find any traces on disk

- Initial experiments on the Pi
  - Imitate general user activity – browse the internet, download files, create/delete files on disk.
  - Use USB storage device(s)
  - Analyse SD Card images to find evidence and/or artefacts

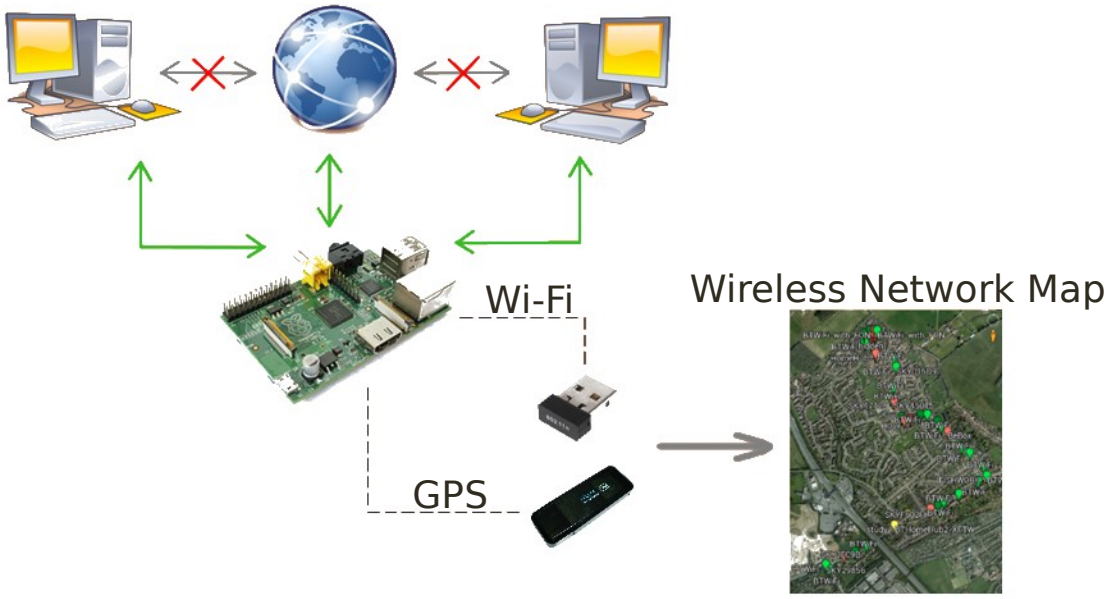


Project – Wireless Sniffing

Aim

- *Establishing the potential forensic artefacts recoverable from a Raspberry Pi device.*

Picture

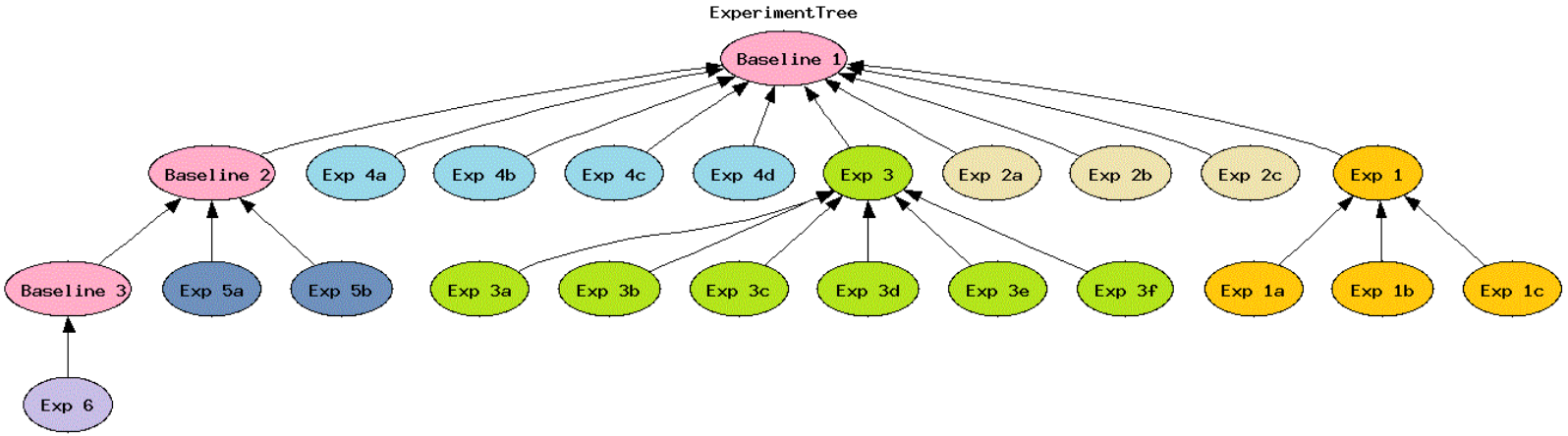


Cranfield UNIVERSITY
Centre for Forensic Computing

Methodology

- Preliminary research – file system analysis and experiments
- OS comparison – Raspbian vs. Arch vs. RISC vs. PwnPi vs. Kali
- Closed LAN Experiments
  - Network mapping
  - Packet sniffing
- ‘The Final Phase’ – moving on to wireless networks
  - Designing an experimental plan
  - Evaluating the experimental and analysis plan
  - Conducting experiments and analysis

Experiments



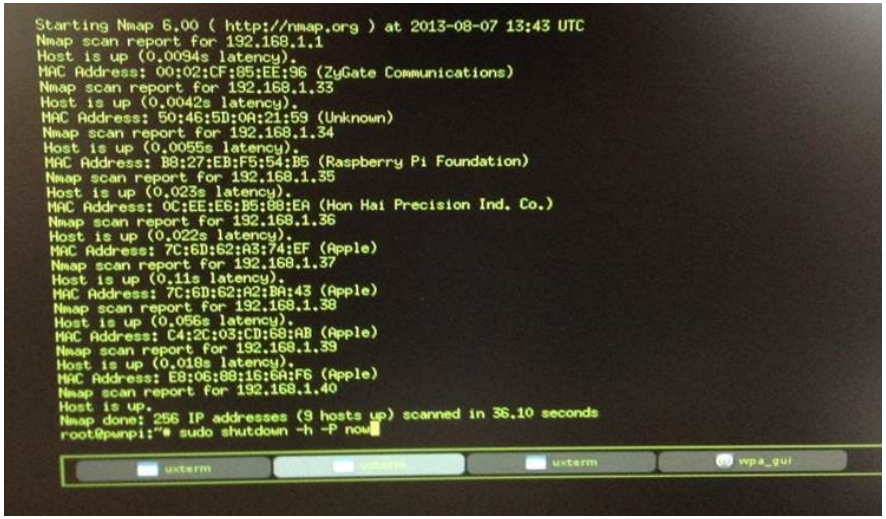
- Experiments included:
  - Exp 1* - Network mapping
  - Exp 2* - DoS attacks
  - Exp 3* - Packet sniffing
  - Exp 4* - Wireless encryption cracking
  - Exp 5* - GPS use
  - Exp 6 - Final Project – GPS + WiFi

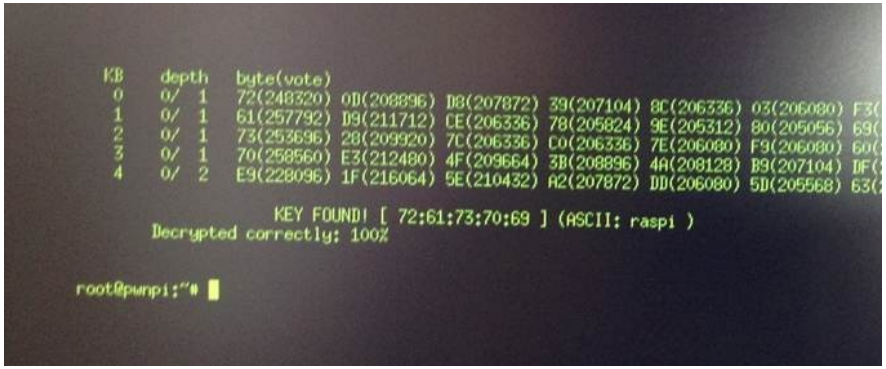
- The tree was designed to minimize variables between each experiment.
- A node with children was not wiped.
- A node without children was wiped with its parents' image.

Cranfield UNIVERSITY
Centre for Forensic Computing

Results

- Network mapping ✔
- DoS attacks ✔
- Packet sniffing ✔
- Wireless encryption cracking
  - WEP ✔
  - WPA/WPA2 ✘
- GPS ✔
- GPS + WiFi ✔





Cranfield UNIVERSITY
Centre for Forensic Computing

Thank You.

Cranfield UNIVERSITY
Centre for Forensic Computing