

# Digital forensic analysis of the Raspberry Pi

Dhruv M. Saxena, Delhi Technological University,  
[dhruvmsaxena@gmail.com](mailto:dhruvmsaxena@gmail.com)

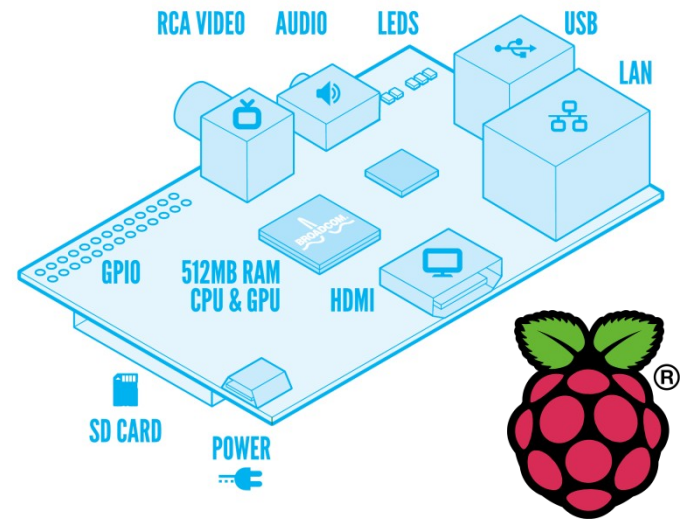
**Supervisor:** Dr. Sarah Morris, Centre for Forensic Computing

# 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

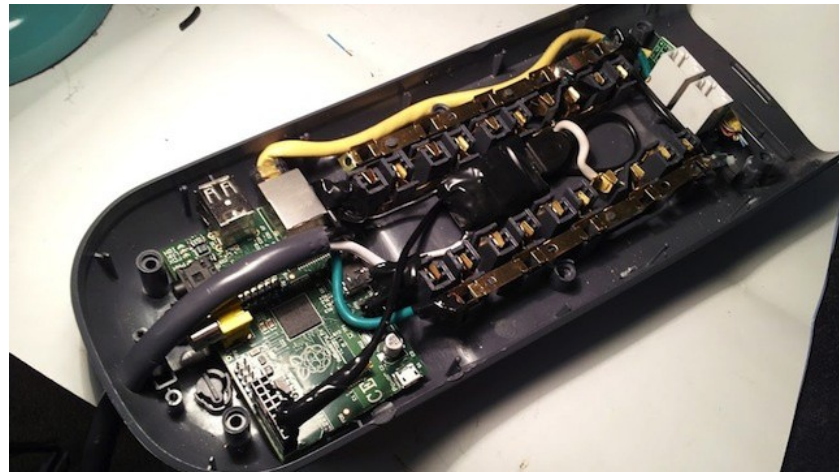
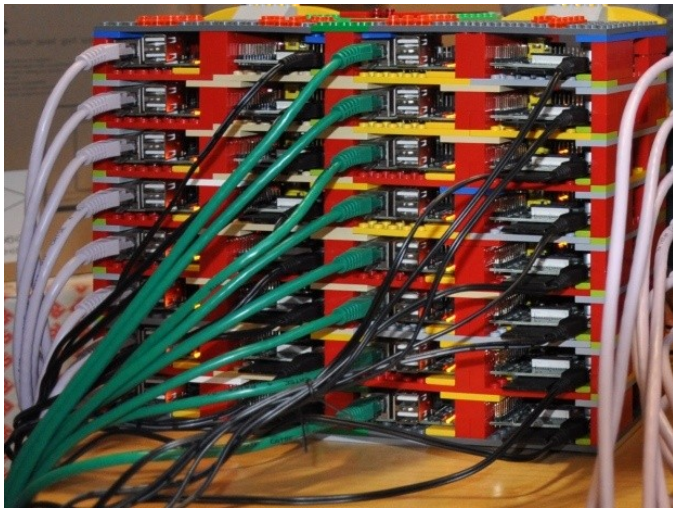
# Raspberry Pi

- 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

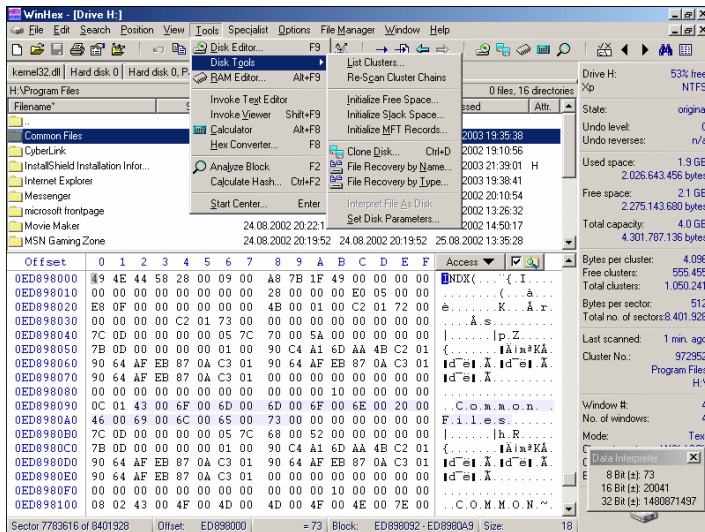


# Getting Started with Digital Forensics

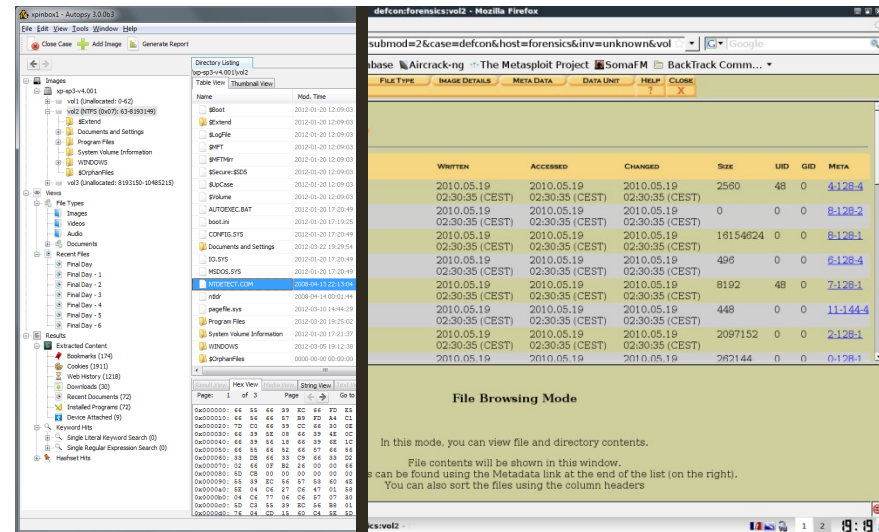
- Reading
  - ACPO Guidelines
  - Search and Seizure
- Test Case – Money Fraud
  - Used WinHex
  - Analysis of image(s)
  - Documentation
- Literature Review – for journal paper
- Python scripts
  - To compare images – baseline vs. experiment
  - To generate a HTML report
    - Of the comparison results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

# Getting Started with Digital Forensics

- Software



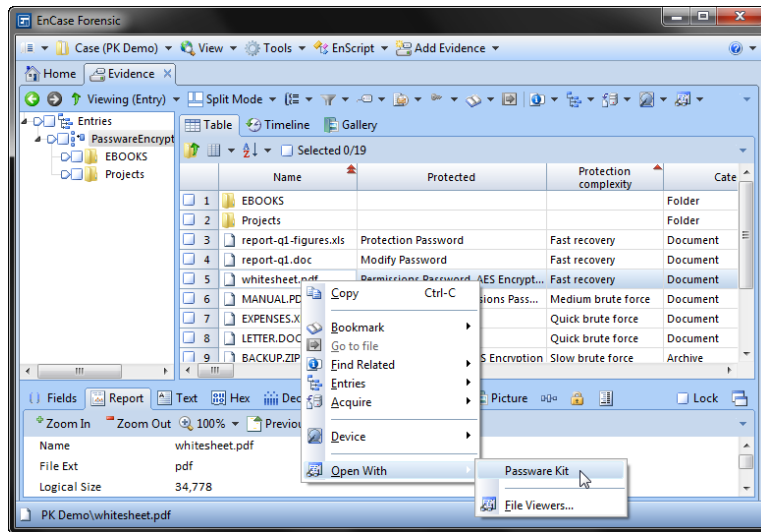
WinHex



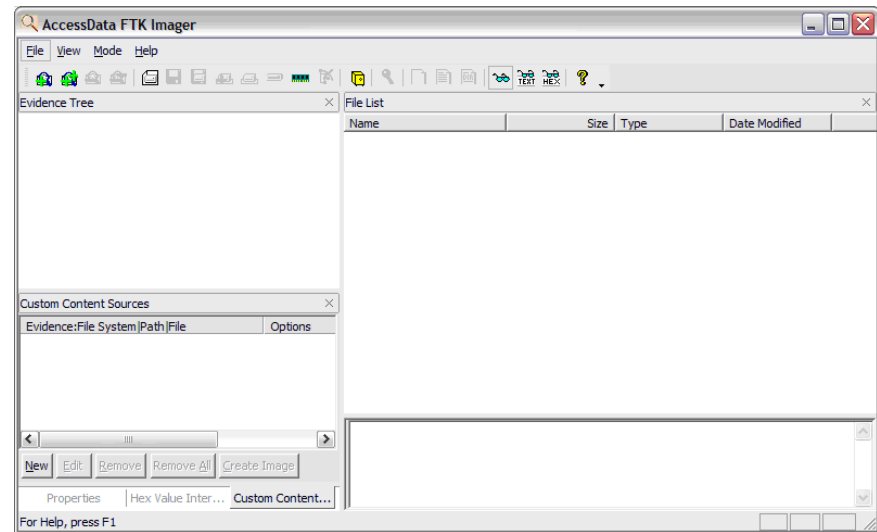
Autopsy for Windows/Linux  
(based on The Sleuth Kit)

# Getting Started with Digital Forensics

- **Software (contd.)**



EnCase

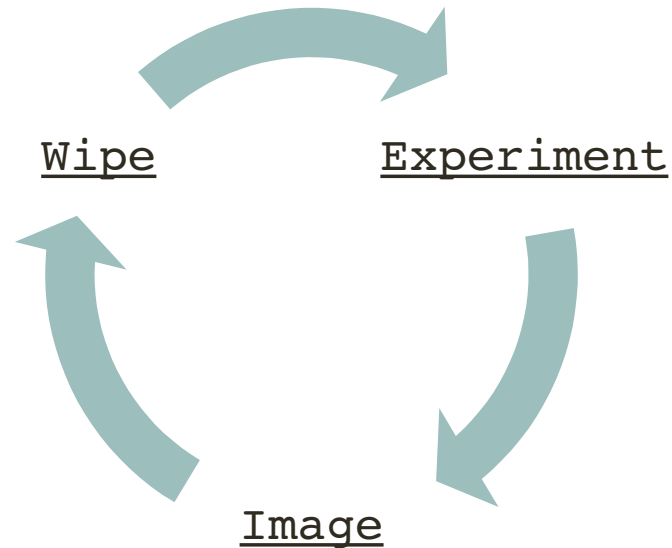


AccessData FTK Imager



# 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



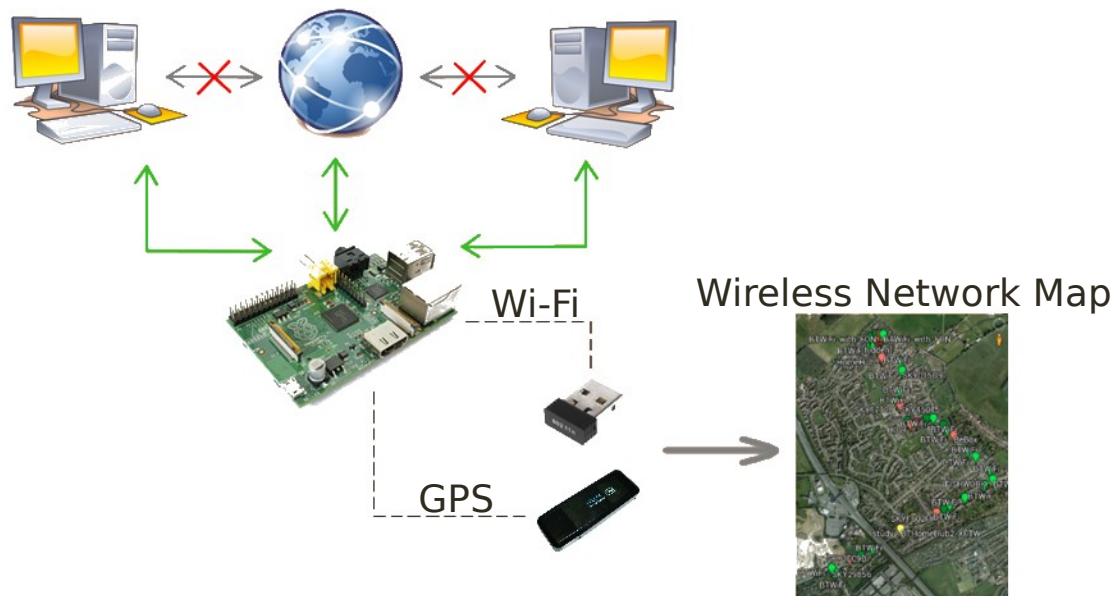


# Project – Wireless Sniffing

## Aim

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

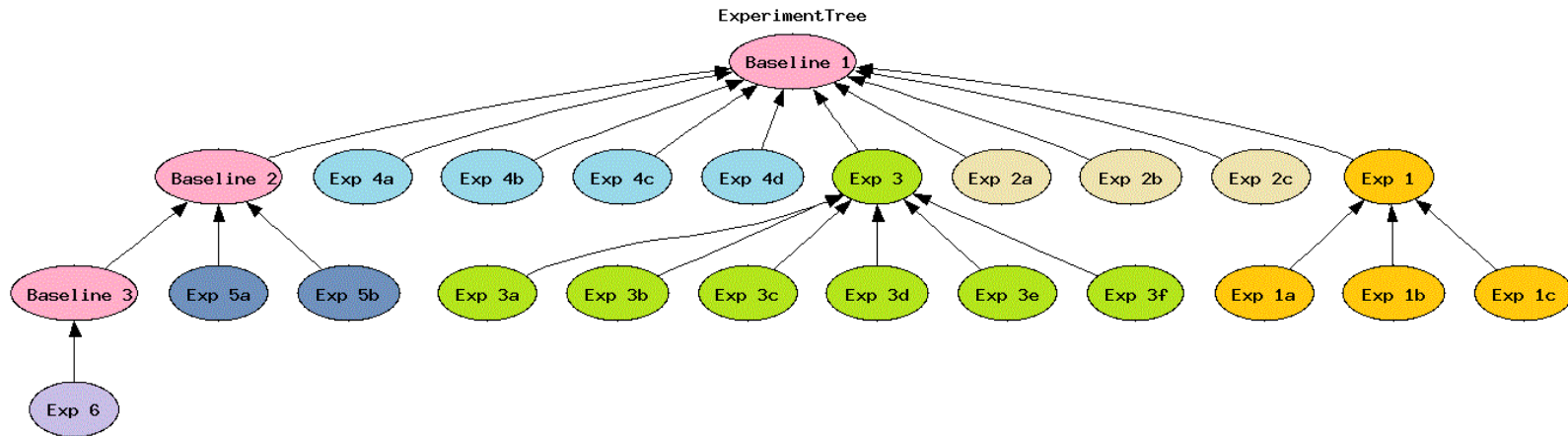
## Picture



# 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.

# Results

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

```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-08-07 13:43 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0094s latency).
MAC Address: 00:02:CF:85:EE:96 (ZyGate Communications)
Nmap scan report for 192.168.1.33
Host is up (0.0042s latency).
MAC Address: 50:46:5D:0A:21:59 (Unknown)
Nmap scan report for 192.168.1.34
Host is up (0.0055s latency).
MAC Address: B8:27:EB:F5:54:B5 (Raspberry Pi Foundation)
Nmap scan report for 192.168.1.35
Host is up (0.023s latency).
MAC Address: 0C:EE:EG:B5:88:EA (Hon Hai Precision Ind. Co.)
Nmap scan report for 192.168.1.36
Host is up (0.022s latency).
MAC Address: 7C:6D:62:A3:74:EF (Apple)
Nmap scan report for 192.168.1.37
Host is up (0.11s latency).
MAC Address: 7C:6D:62:A2:1A:43 (Apple)
Nmap scan report for 192.168.1.38
Host is up (0.056s latency).
MAC Address: C4:2C:03:CD:68:AB (Apple)
Nmap scan report for 192.168.1.39
Host is up (0.018s latency).
MAC Address: E8:06:88:16:6A:F6 (Apple)
Nmap scan report for 192.168.1.40
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 36.10 seconds
root@punpi:~# sudo shutdown -h -P now
```

```
KB depth byte(vote)
0 0/ 1 72(248320) 0D(208896) D8(207872) 39(207104) 8C(206336) 03(206080) F3(
1 0/ 1 61(257792) D9(211712) CE(206336) 78(205824) 9E(205312) 80(205056) 89(
2 0/ 1 73(253696) 28(209920) 7C(206336) C0(206336) 7E(206080) F9(206080) 60(
3 0/ 1 70(258560) E3(212480) 4F(209664) 3B(208896) 4A(208128) B9(207104) DF(
4 0/ 2 E9(228096) 1F(216064) 5E(210432) A2(207872) DD(206080) 5D(205568) 63(

KEY FOUND! [ 72:61:73:70:69 ] (ASCII: raspi )
Decrypted correctly: 100%

root@punpi:~#
```

Thank You.