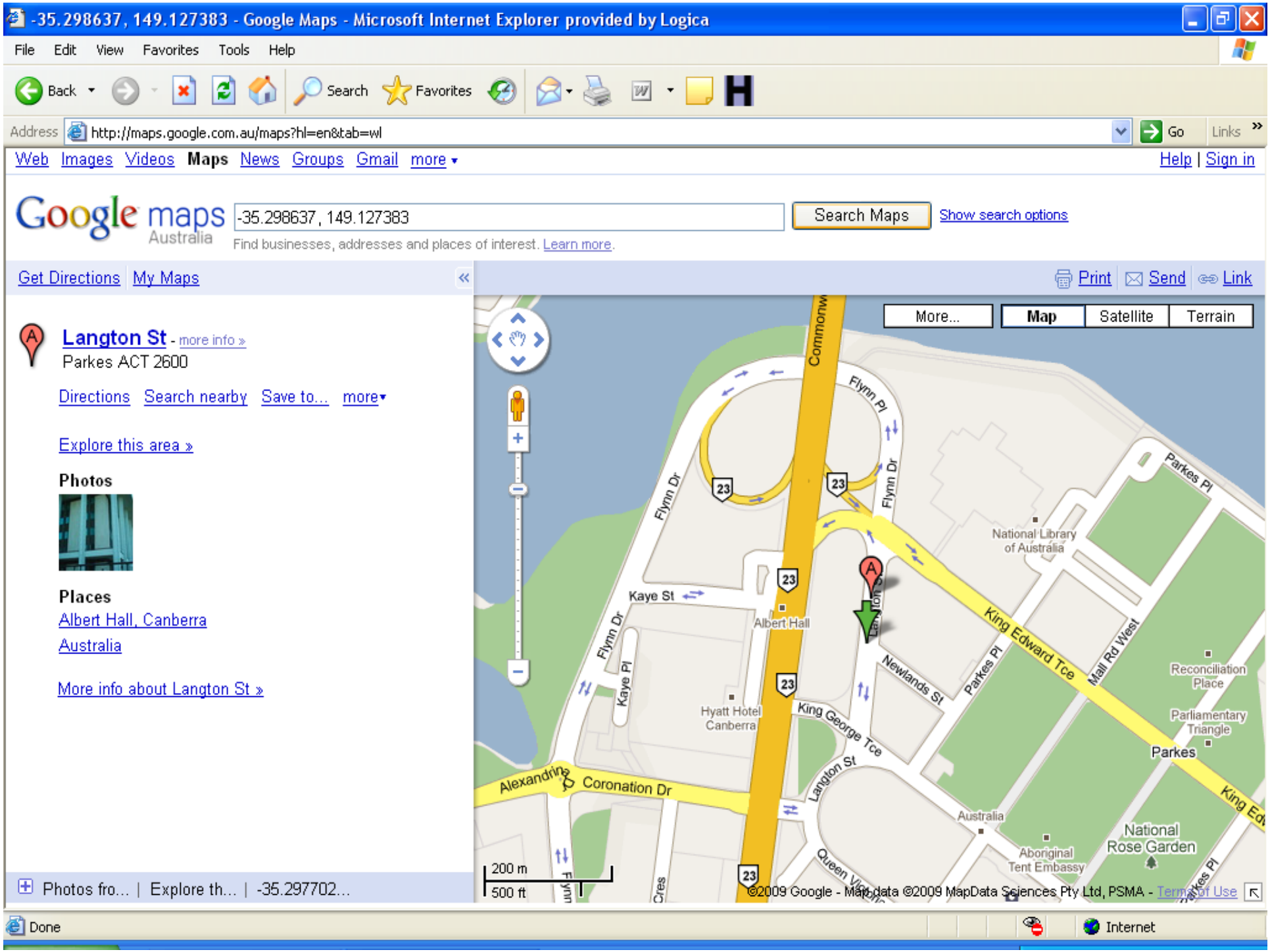
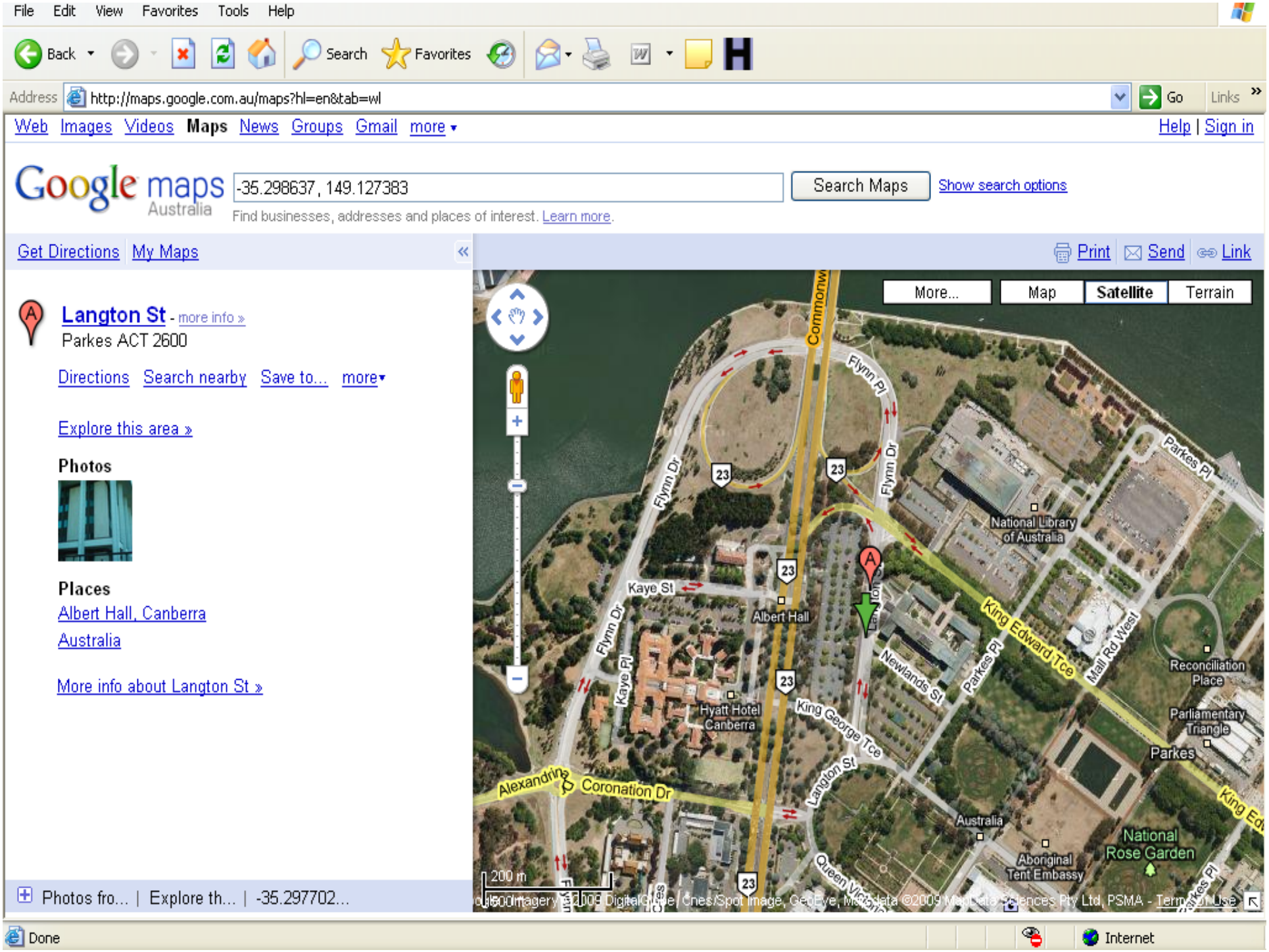
Metadata in photographs

- A media organisation received e-mail with link to photographs of public-interest documents published on the Internet
- All “normal” identity data resolved to an Internet café
- Examined EXIF metadata and found that the pictures were taken using iPhone
- Geocoding confirmed that pictures were taken inside XXXX. Other pictures revealed a home and thence the person “leaking” the documents
- EXIF fields of interest:
  - GPS latitude
  - GPS longitude
  - GPS position e.g. S35° 18.0283', E149° 7.5934'


-35.298637, 149.127383 - Google Maps - Microsoft Internet Explorer provided by Logica
File Edit View Favorites Tools Help
Back Search Favorites
Address http://maps.google.com.au/maps?hl=en&tab=wl
Go Links
Web Images Videos Maps News Groups Gmail more
Help | Sign in
Google maps Australia
-35.298637, 149.127383
Search Maps
Show search options
Find businesses, addresses and places of interest. Learn more.
Get Directions My Maps
Print Send Link
Langton St - more info »
Parkes ACT 2600
Directions Search nearby Save to... more
Explore this area »
Photos
Places
Albert Hall, Canberra
Australia
More info about Langton St »
More... Map Satellite Terrain
Commonwealth Ave
Flynn Pl
Flynn Dr
Kaye St
Kaye Pl
Albert Hall
Hyatt Hotel Canberra
King George Tce
Newlands St
Parkes Pl
National Library of Australia
King Edward Tce
Mall Rd West
Reconciliation Place
Parliamentary Triangle
Parkes
Alexandrina Dr
Coronation Dr
Langton St
Australia
Aboriginal Tent Embassy
National Rose Garden
Queen Victoria Terrace
Cres
23
200 m
500 ft
©2009 Google - Map data ©2009 MapData Sciences Pty Ltd, PSMA - Terms of Use
Photos fro... | Explore th... | -35.297702...
Done
Internet


File Edit View Favorites Tools Help
Back Search Favorites
Address http://maps.google.com.au/maps?hl=en&tab=wl
Go Links
Web Images Videos Maps News Groups Gmail more
Help | Sign in
Google maps Australia
-35.298637, 149.127383
Search Maps
Show search options
Find businesses, addresses and places of interest. Learn more.
Get Directions My Maps
Print Send Link
Langton St - more info »
Parkes ACT 2600
Directions Search nearby Save to... more
Explore this area »
Photos
Places
Albert Hall, Canberra
Australia
More info about Langton St »
More... Map Satellite Terrain
Commonwealth Ave
Flynn Pl
Flynn Dr
Parkes Pl
National Library of Australia
Kaye St
Albert Hall
King Edward Tce
Mall Rd West
Reconciliation Place
Newlands St
Kaye Pl
Hyatt Hotel Canberra
King George Tce
Parliamentary Triangle
Parkes
Alexandrina
Coronation Dr
Langton St
Australia
Aboriginal Tent Embassy
National Rose Garden
Queen Victoria Terrace
200 m
Photos fro... | Explore th... | -35.297702...
Done
Internet


Map
Satellite
Hybrid
Google
Imagery ©2009 DigitalGlobe, GeoEye - Terms of Use

Hash functions

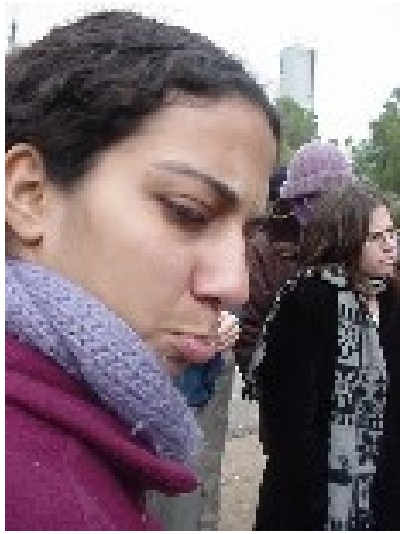
- The chance of two different files generating the same MD5 hash or “digital fingerprint” is 2^{128} with one in 2^{32} chance of collision
- The chance of two different files generating the same SHA1 hash or “digital fingerprint” is 2^{160} with one in 2^{69} chance of collision
- To put this in context:
  - the Galton study suggests that the chances of any two human beings having the same fingerprint is one in 6,400,000,000
  - or Osterburg study suggests that the chances of any two human beings having the same fingerprint is one in 100,000,000,000,000,000.

2^{32} = 4,294,967,296
2^{40} = 1,099,511,627,776
2^{69} = 590,295,810,358,705,651,712
6,400,000,000
100,000,000,000,000,000

Don’t rely on hash sets for finding pictures...

SUCKOFF.JPG


Keep back from
the platform edge
or you may get sucked off
Penrith



Sufficiency

- Prosecution has an obligation to make reasonable effort to discover both incriminating and exculpatory evidence

- Is the evidence copy complete? Is it missing bits? Is the missing bit(s) relevant?

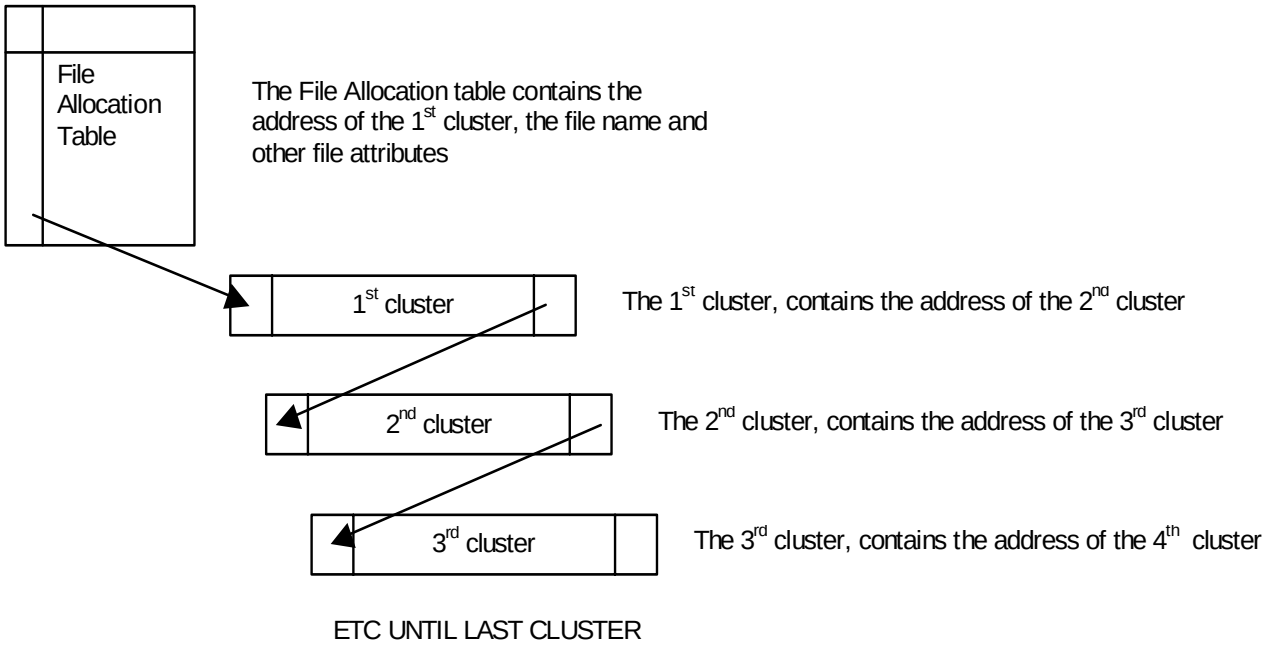
  - `The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The256ick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick brown fox jumps over the lazy grey dog. The quick512`

- Does the Police examiner understand that bits are missing?
  - New hardware skips sectors on old disks
  - A popular forensic software fails to copy the last sector of a disk when there are an odd number of sectors
  - The statistical failure rate can be significant

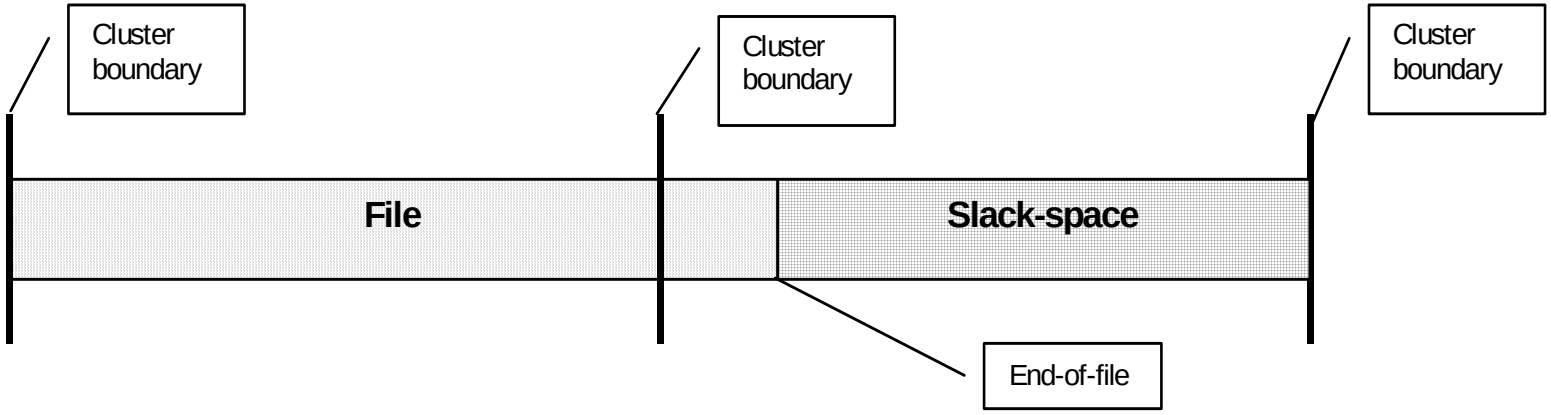
- Can they prove the person did it?
  - Its not good enough to prove the computer did it

Standard Recovery Techniques

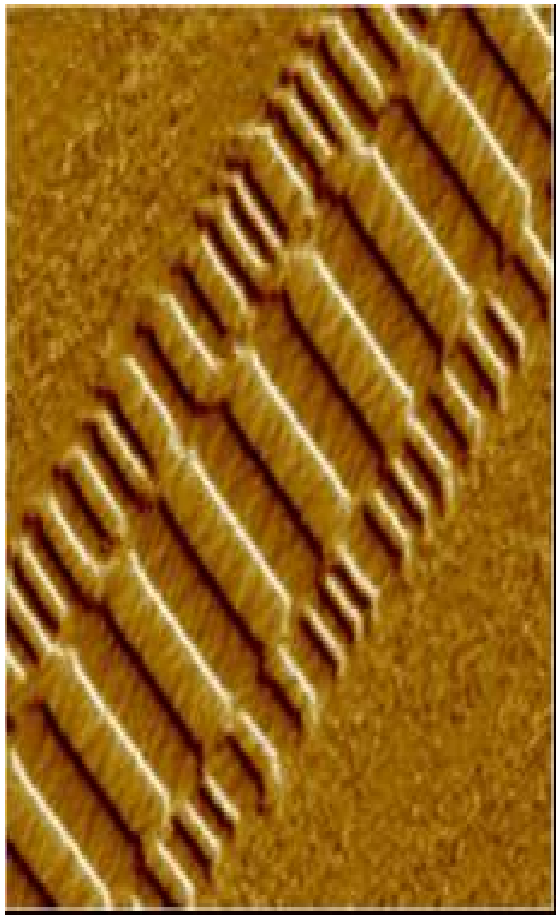
- When a program wants to access a file, it is assisted by the operating system, which looks for the file name in the FAT. It then uses the corresponding address to find the 1st cluster. After reading the 1st cluster, it uses the address of the 2nd cluster to find the 2nd cluster. After reading the 2nd cluster, it uses the address of the 3rd cluster to find the 3rd cluster and so forth until the end of the file.



- A hard disk is logically grouped in clusters and the start of a file is always the start of a cluster. A file will typically span more than one cluster, however the end-of-file (i.e. ‘EOF’) marker may not match a cluster boundary. Thus there may be some space between the end-of-file and the next cluster boundary. This is called ‘slack space’ and may contain data belonging to a previously deleted file.

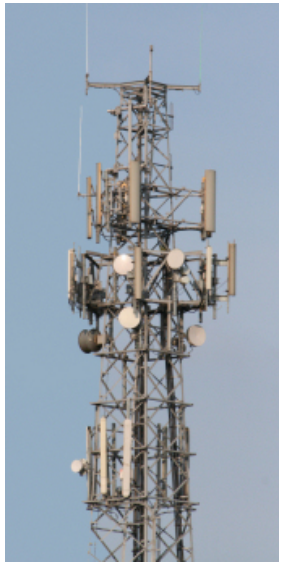


Advanced recovery techniques



- This is an image of the platter of a hard disk that has been enhanced by an electron microscope.
- A single track is prominent in the centre of the illustration. This is the image of the electrical impulses recorded on the hard disk and constitutes the currently written file. As the platter spins, the impulses are recorded onto the platter by a tiny motor-controlled head, forming concentric tracks on the media.
- In this illustration, the current data consists of “01010101010101010101” that visualize as alternate ridges and valleys
- Only relevant for older disks
- Expensive (~$120k per 5Gb)

Mobile phones



Two aspects:

1.What is on the phone (really it’s just another computer):

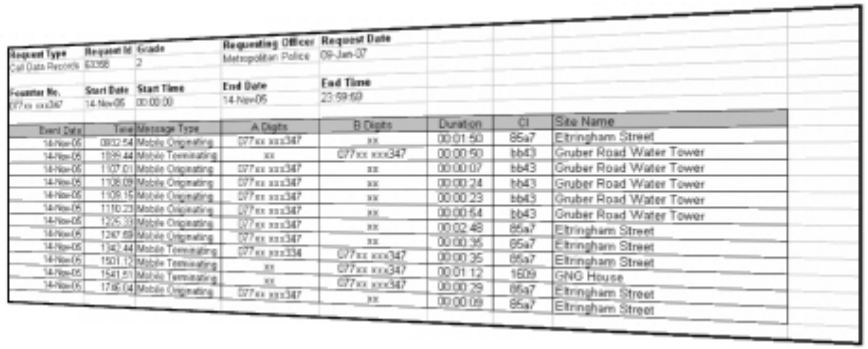
- Messages
- Pictures & video
- Contacts

2.Where was the phone

- Where was the person?

Key issues:

- Location (which cell?)
- Was the message read?
- When/where was a photograph taken?



Request Type	Request Id	Grade	Requesting Officer	Request Date
Call Data Records	53398	2	Metropolitan Police	09-Jan-07

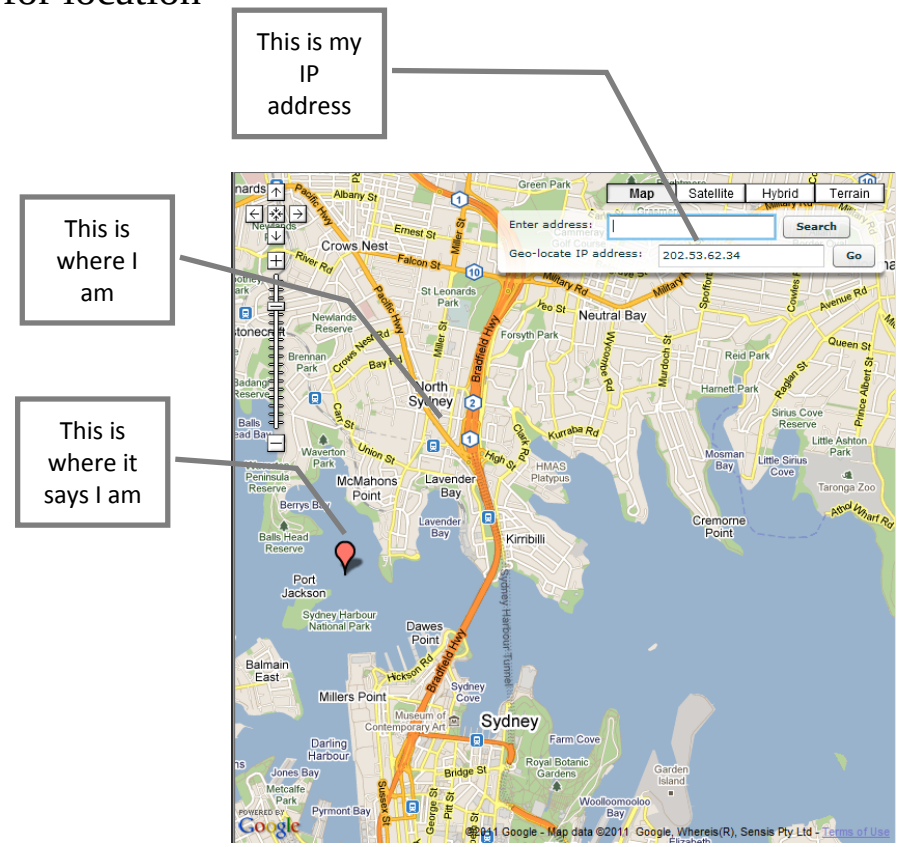
Counter No.	Start Date	Start Time	End Date	End Time
077xx xxx347	14-Nov-05	00:00:00	14-Nov-05	23:59:59

Event Date	Time	Message Type	A Digits	B Digits	Duration	CI	Site Name
14-Nov-05	0802:54	Mobile Originating	077xx xxx347	xx	00:01:50	86a7	Eltringham Street
14-Nov-05	1899:44	Mobile Terminating	xx	077xx xxx347	00:00:50	bb43	Gruber Road Water Tower
14-Nov-05	1107:01	Mobile Originating	077xx xxx347	xx	00:00:07	bb43	Gruber Road Water Tower
14-Nov-05	1108:09	Mobile Originating	077xx xxx347	xx	00:00:24	bb43	Gruber Road Water Tower
14-Nov-05	1109:15	Mobile Originating	077xx xxx347	xx	00:00:23	bb43	Gruber Road Water Tower
14-Nov-05	1110:23	Mobile Originating	077xx xxx347	xx	00:00:54	bb43	Gruber Road Water Tower
14-Nov-05	1245:39	Mobile Originating	077xx xxx347	xx	00:02:48	86a7	Eltringham Street
14-Nov-05	1247:59	Mobile Originating	077xx xxx347	xx	00:00:35	86a7	Eltringham Street
14-Nov-05	1357:44	Mobile Terminating	077xx xxx334	077xx xxx347	00:00:35	86a7	Eltringham Street
14-Nov-05	1501:17	Mobile Terminating	xx	077xx xxx347	00:01:12	1609	GNG House
14-Nov-05	1541:51	Mobile Terminating	xx	077xx xxx347	00:00:29	86a7	Eltringham Street
14-Nov-05	1746:04	Mobile Originating	077xx xxx347	xx	00:00:09	86a7	Eltringham Street

Understand what location service your “phone” is using

- New devices don’t always use towers for location
  - Wi-Fi access points
  - GPS
  - ...and then phone tower

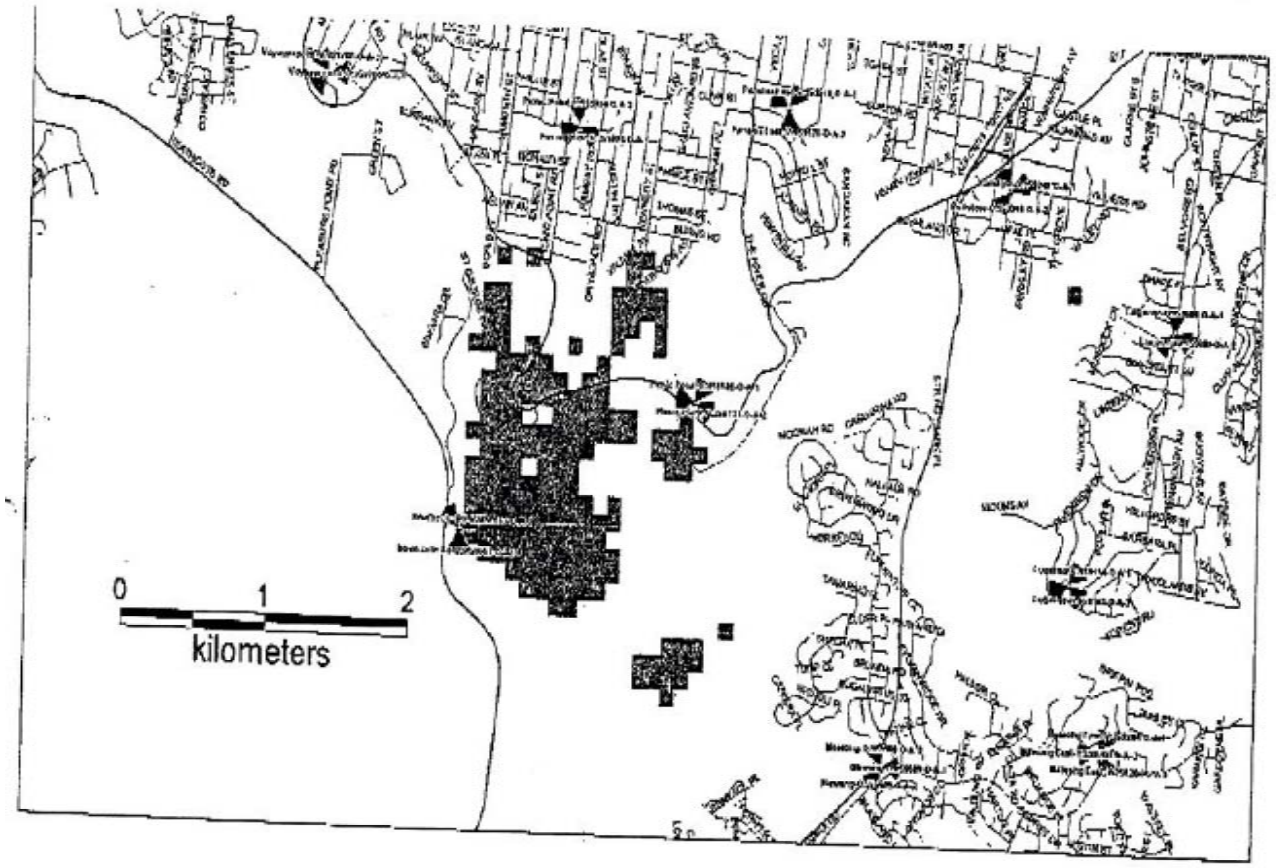
- Other locations service:
  - Skyhook
  - Google



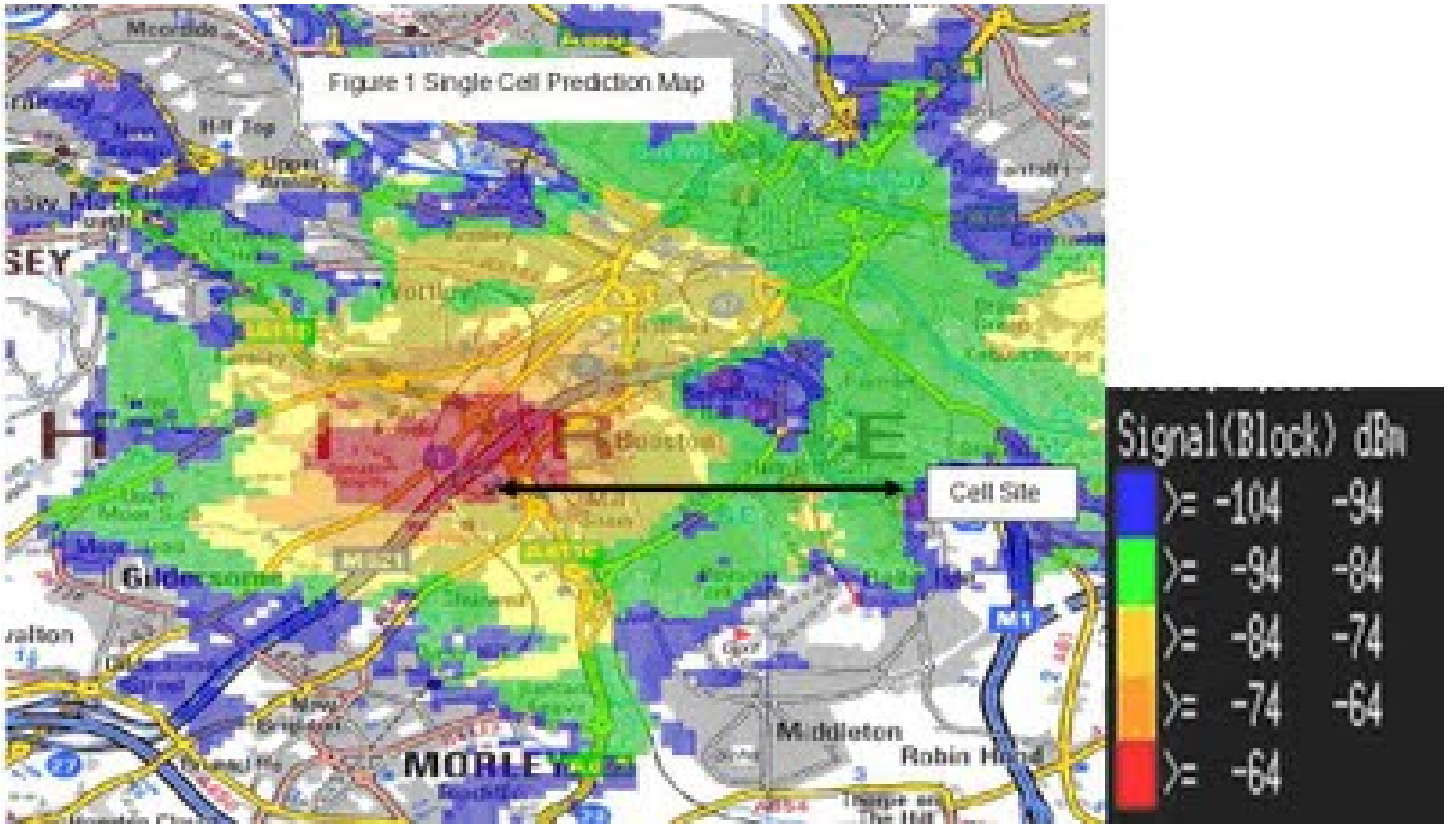
Police and telcos typically use “best tower” method

- ...but it is circumstantial and depends on:
  - Whether the handset is stationary or moving (i.e. In car)
  - Topography
  - Transient features eg:
    - Weather
    - Airplane, rail, truck

Figure 1: Plot showing Prediction of Probable Cell Coverage area for Heathcote Rd_1 (Shaded)



...but it’s flawed because...



The BSS list

- The BSS-list measures surrounding cells
  - It can be used to establish that the serving cell was not the nearest cell

- You could so the same on your HTC or Motorola...if you went to the site

Thank you

ajoy.ghosh@optusnet.com.au