UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 8

5 November 2019

Topics for this lecture

Telecommunications data and metadata

- Gathering telecommunications data/metadata (slides)
- Hands on exercise – locating the accused from telco data (from my laptop)

Be clear of your right to access the phone (without warrant)

PRINCIPLE

The person or entity that legally owns the phone is the only person who can authorise access to the phone, except if access it illegal

- Access to the phone and data stored <u>on</u> the phone
- Those legally entitled to act on the owner's behalf
- Different to authorising access to <u>communications</u> (only the recipient)[1]
- Different to data accessed <u>from</u> the phone

1. §6 of Telecommunication (Interception and Access) Act 1979

- Cannot authorise illegal access
  - The Court does have discretion to admit evidence on the basis of natural justice or public interest
- Other prohibited access e.g.
  - Workplace surveillance
  - Court Orders – Family Court orders preventing access are common
  - No general exemption to possess illegal content or sensitive evidence
- Exceptions prevent disclosure
  - Privilege
  - Self incrimination

} Usually apply to the giving of the data to someone else

Be clear of your right to access “communications”

- Communication[1]

  includes conversation and a message, and any part of a conversation or message, whether:

  (a) in the form of:

  (i) speech, music or other sounds;

  (ii) data;

  (iii) text;

  (iv) visual images, whether or not animated; or

  (v) signals; or

  (b) in any other form or in any combination of forms.

- Stored communication[2]

means a communication that

(a) is not passing over a telecommunications system; and

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and

(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

- Telecommunications interception[3]

  interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

⇩

- Be clear about “telecommunications system” and “carrier”

1. and 2. Definitions in Telecommunication (Interception and Access) Act 1979

3.§6 of Telecommunication (Interception and Access) Act 1979

Activity

For the following scenarios, discuss:

1. Can your client authorise you to access the relevant data?
2. What steps would you take to clarify your right to access: (a) the phone (b) the data on the phone, and (c) the data accessed from the phone

Workplace

- Your client is the HR manager of a SME business
- Your client gives you an iPhone and wants you to examine it for workplace harassment via email and instant message
- The iPhone belongs to the business and was allocated to a worker Ajoy Ghosh, against whom a complaint has been made
- Your client tells you the PIN has been reset to 0000
- You observe that the iCloud account being used is ajoy.ghosh@icloud.com

My old device

- Your client, the CEO, wants you to extract old SMS messages from an iPhone 8 and gives you the device and its PIN. The relevant data is 1½ years old
- Your client explains that it belongs to the business. It used to be used by himself and when he got an iPhone X, he gave it to his child to use. The child lives with their mother
- You are aware that the old emails relate to a significant legal case and getting it tip the case in your client's favour

Agency

- Your client is the in-house lawyer for an agency who gives you an agency laptop which was being used by a former staff member
- She asks you to find evidence that the former staffer was sending messages to a journalist in the weeks prior to their leaving
- You discover a Kies backup archive – you know the Agency has a BYO policy and does not issue mobile phones
- You see that there is no password for the Kies backup

Telco vs Data

- Calls
- SMS
- MMS
- iMessage, WhatsApp
- Email
- Contacts
- Location

- Insights come from unfusing telco and data records and then fusing them again and against other data
  - If you can get the telco data
- Data doesn't match a surprising number of times

⇩

Reliable?

Sufficient?

Spoiled or Tampered?

Onus of proof

- The onus of proof is on the party seeking to establish that ***outcome produced by a process, machine or device*** is unreliable
- Standard of proof depends on whether your testimony is being called by prosecution or defendant (remember "*there is no ownership in the testimony of an expert*"[1])

⇩

- Once that is established, the onus is on the party relying on the "outcome" to prove it is reliable

- Always provide testimony regarding the reliability of your own evidence
  1. Your own testing of the particular process
  2. Your prior experience and the experience of your peers
  3. Relevant research

1. Argument of Margret Cunneen SC when seeking to use mobile phone evidence

Sources of data

- The phone
  - The device or an “extraction”
  - A backup (which may be on a computer or the cloud)
  - Surveillance software, spyware or malware
- The telco
  - Call Charge Record
  - Mandatory data retention
  - Monthly account
  - Intercept
- The content provider
  - Sync/backup data
  - Download my data
  - Backup
  - Court order
  - Law enforcement assistance
- The recipient(s)
- Data communications e.g. wireless access point

DISCUSSION

If someone else has compromised the phone, is it okay to use the resulting data?

Telephone, stored communications and MDR

INTERCEPTION & STORED COMMUNICATIONS

- Access some data on request
  - Originating number (A party)
  - Receiving number (B party)
  - Location of A and B party
  - Type of communication
  - Duration

⇩

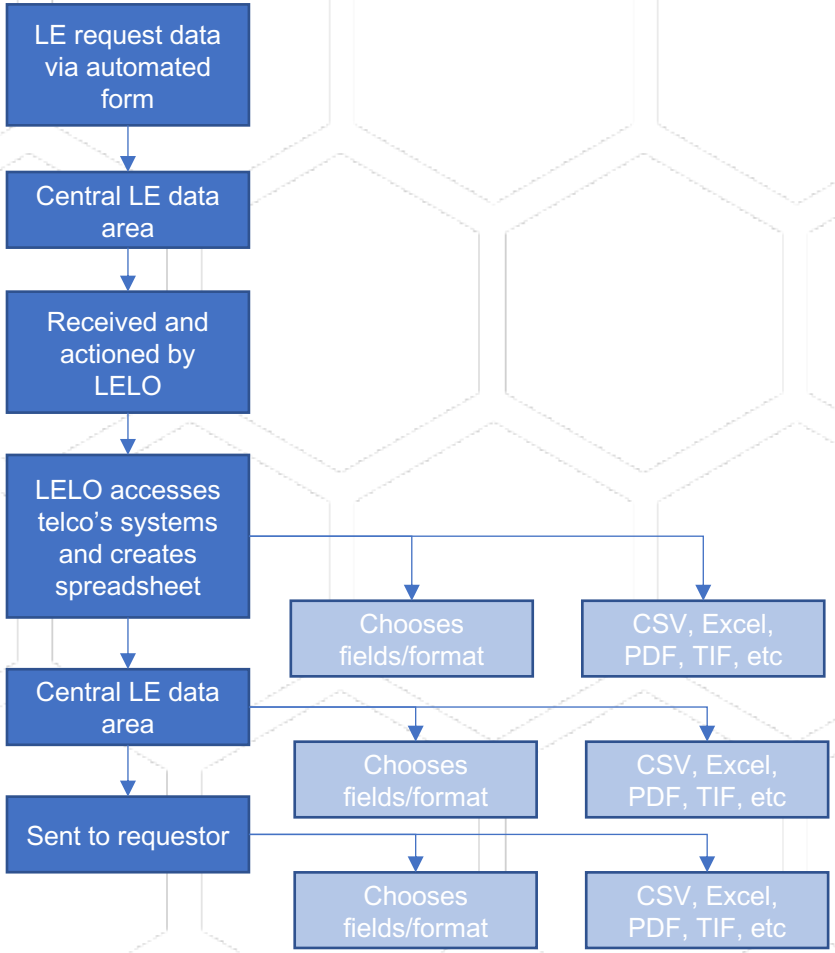
Referred to as Call Charge Record (CCR)

- Access content under warrant
  - e.g. SMS message

MANDATORY DATA RETENTION

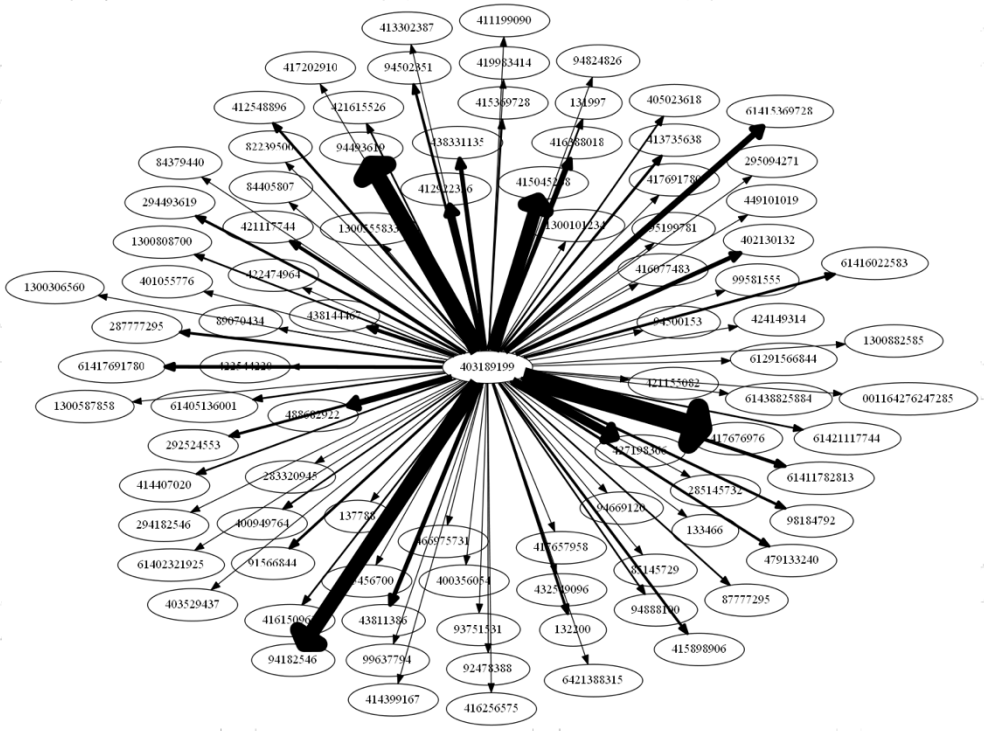
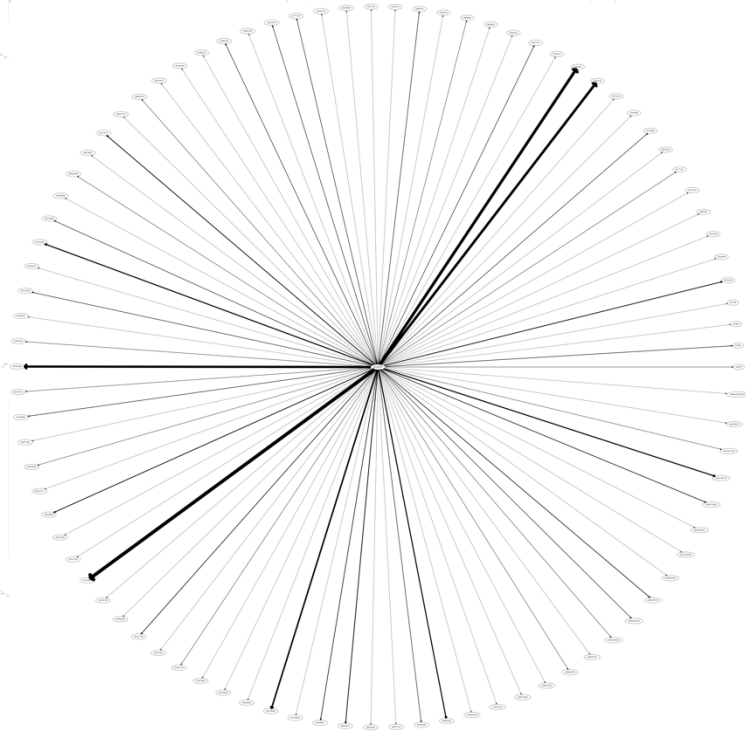
- Since April 2015 telcos and ISP required to store “metadata” for two years
  - Name, address, and billing information
  - Phone number or email, and the phone number or email of the person you're communicating with
  - Time, date and duration of a communication
  - IP address
  - Location of the communication equipment you use; for example, the closest cell tower
  - Type of communication; phone call, text, or email
  - Bandwidth usage such as the amount of data uploaded and downloaded

Creating a CCR



Understand the process

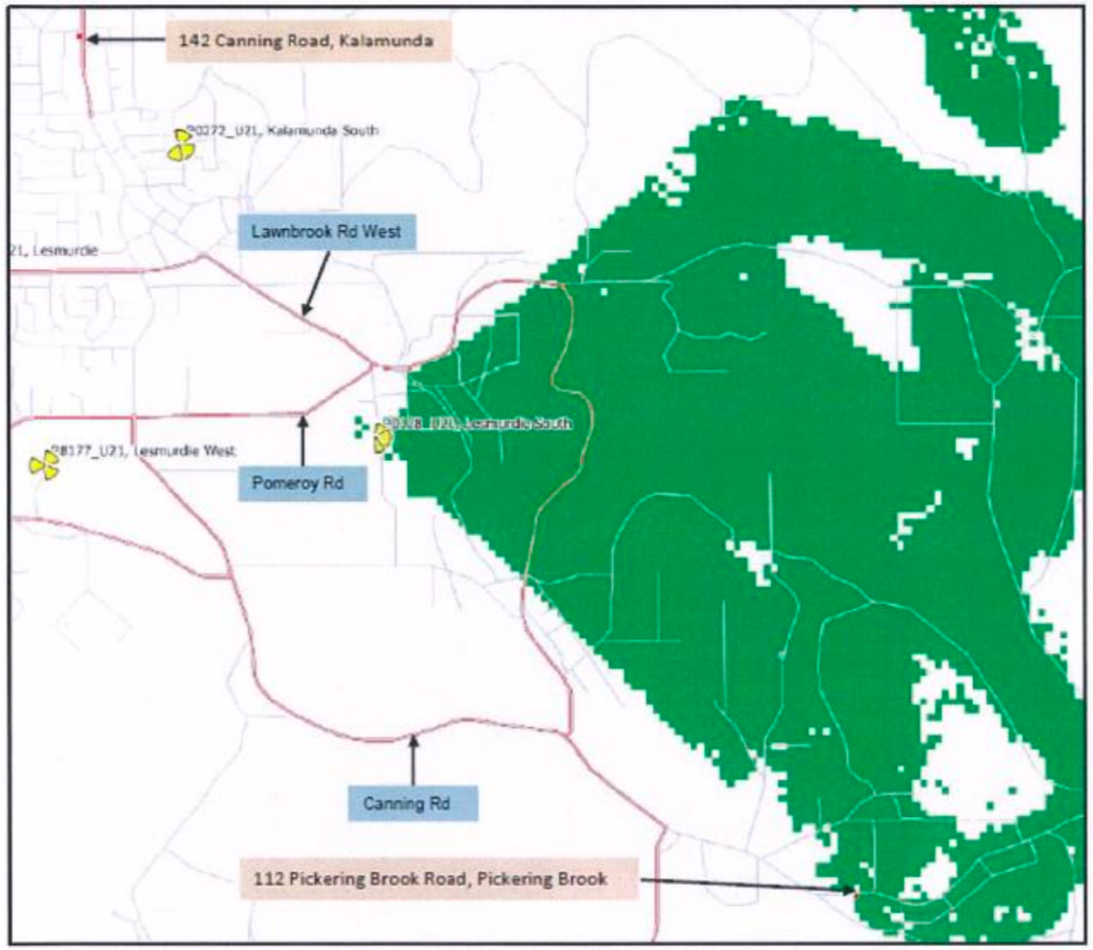
- Each step is an opportunity to:
  - Remove data
  - Change data
  - Add data
- Recall prior example of timestamps
- You may be in the position of having to demonstrate the reliability of the process
- May want o use the data to assist your own examination

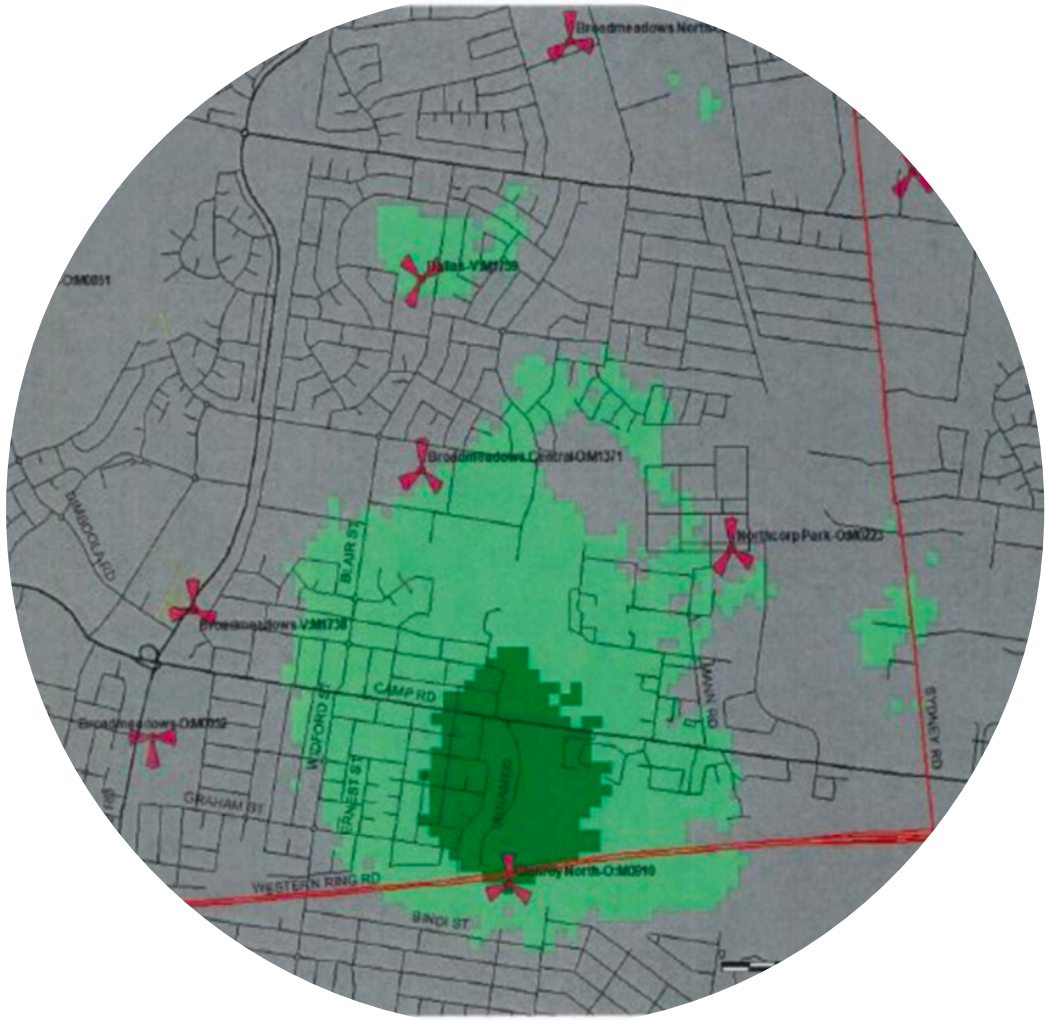

403189199
413302387
411199090
417202910
94502851
419983414
94824826
412548896
421615526
415369728
131997
405023618
61415369728
82239500
94493619
438331135
416988018
413735638
84379440
84405807
415045538
417691780
295094271
294493619
421117744
1300808700
449101019
402130132
422474964
401055776
1300306560
61416022583
99581555
43814446
424149314
287777295
1300882585
61417691780
61291566844
1300587858
61405136001
61438825884
00116427647285
292524553
61421117744
414407020
61411782813
285145732
294182546
137788
98184792
61402321925
91566844
133466
479133240
403529437
456700
87777295
43811386
93751531
132200
415898906
94182546
99637794
92478388
6421388315
414399167
416256575


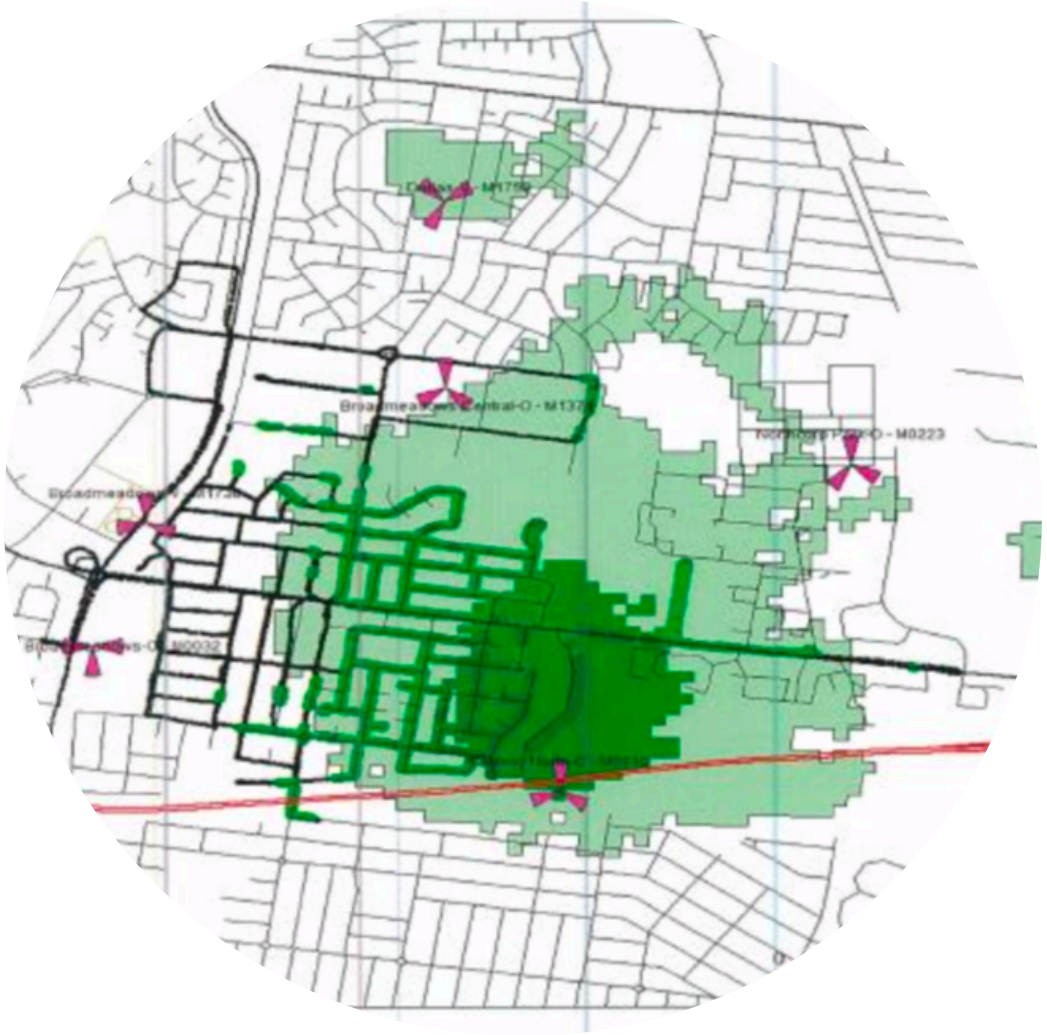
Coverage maps

Probable Coverage (Adelaide Airport)

Possible Coverage (Adelaide Airport)


142 Canning Road, Kalamunda
Lawnbrook Rd West
Pomeroy Rd
Canning Rd
112 Pickering Brook Road, Pickering Brook


BROADMEADOWS
Broadmeadows Central OM1371
Broadmeadows VM1738
Broadmeadows OM1739
Glenroy North-O M0010
CAMP RD
GRAHAM ST
BLAIR ST
WIDFORD ST
ERNEST ST
DIMMOCKS RD
SYDNEY RD
WESTERN RING RD
BINDI ST


Broadmeadows Central-O - M1371