INTRODUCTION TO MOBILE FORENSICS

Dr Matthew Sorell, Principal Consultant and CTO

matthew@digitalforensicsciences.au

Dr Matthew Sorell

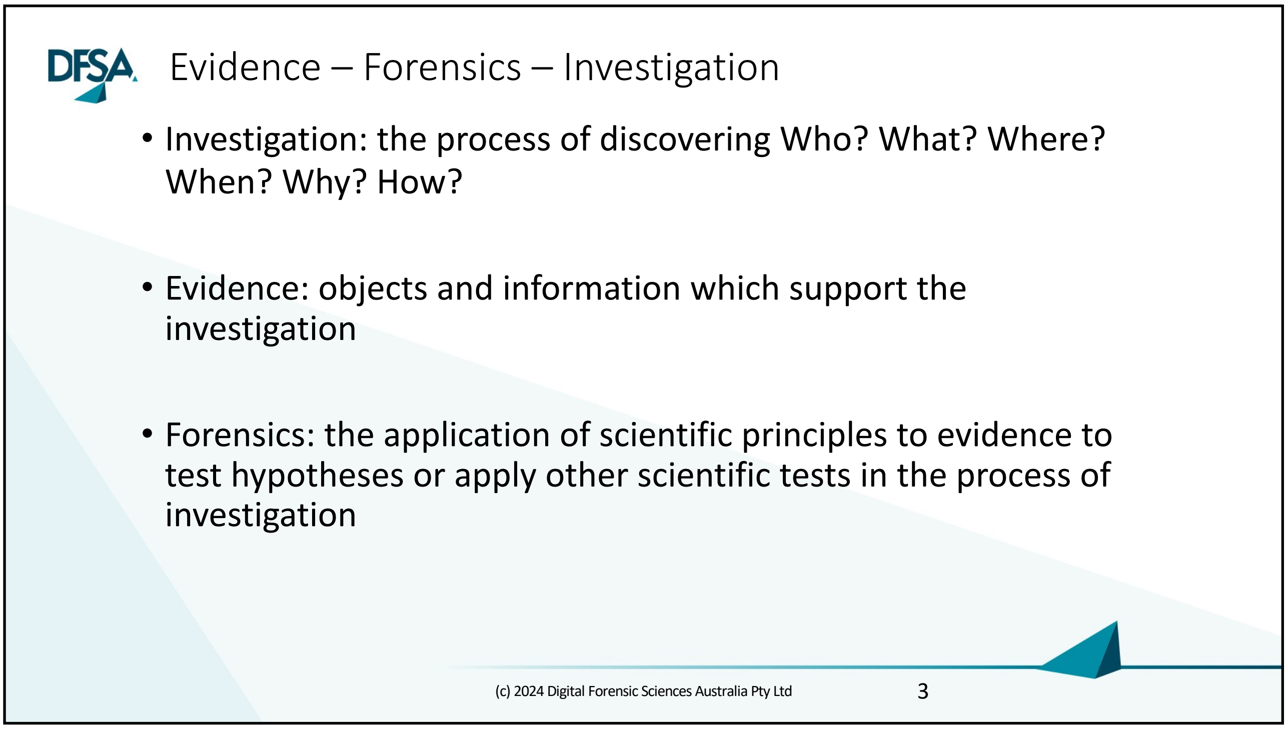
Senior Lecturer, Telecommunications, Multimedia and Digital Forensic Science

Adjunct Professor, Digital Forensic Science

Principal Consultant Director and CTO

Honorary Consul Republic of Estonia in Adelaide

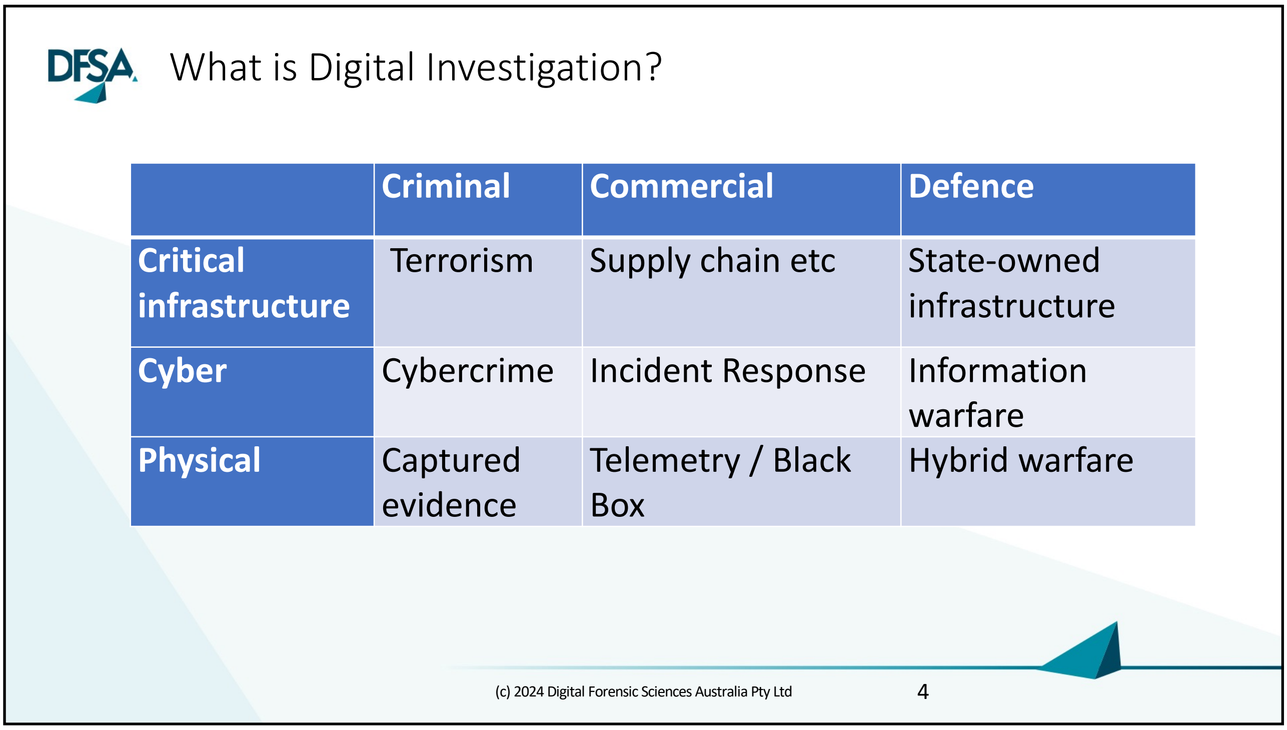
for analysis
~300,000 measurements per year.
인터폴 디지털포렌식 전문가그룹 회의
2nd INTERPOL Digital Forensics Experts Group Meeting



Evidence – Forensics – Investigation

- Investigation: the process of discovering Who? What? Where? When? Why? How?
- Evidence: objects and information which support the investigation
- Forensics: the application of scientific principles to evidence to test hypotheses or apply other scientific tests in the process of investigation

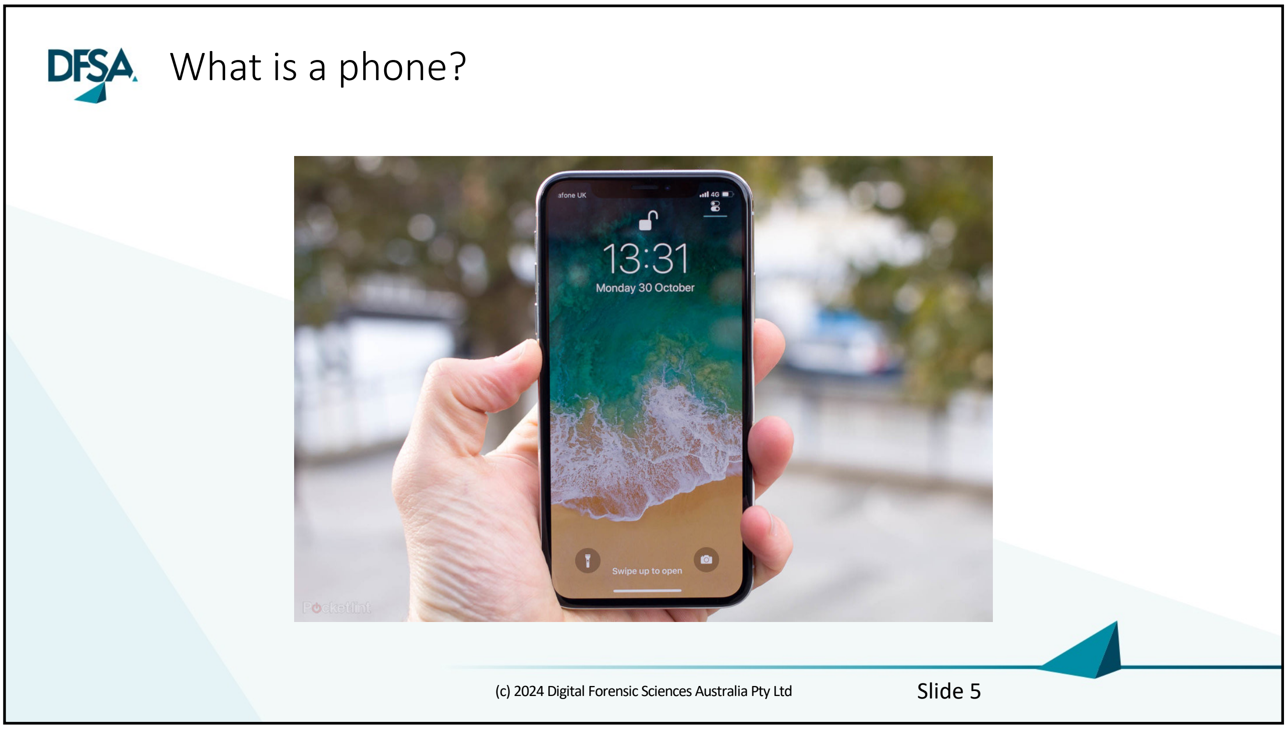
3



What is Digital Investigation?

	Criminal	Commercial	Defence
Critical infrastructure	Terrorism	Supply chain etc	State-owned infrastructure
Cyber	Cybercrime	Incident Response	Information warfare
Physical	Captured evidence	Telemetry / Black Box	Hybrid warfare

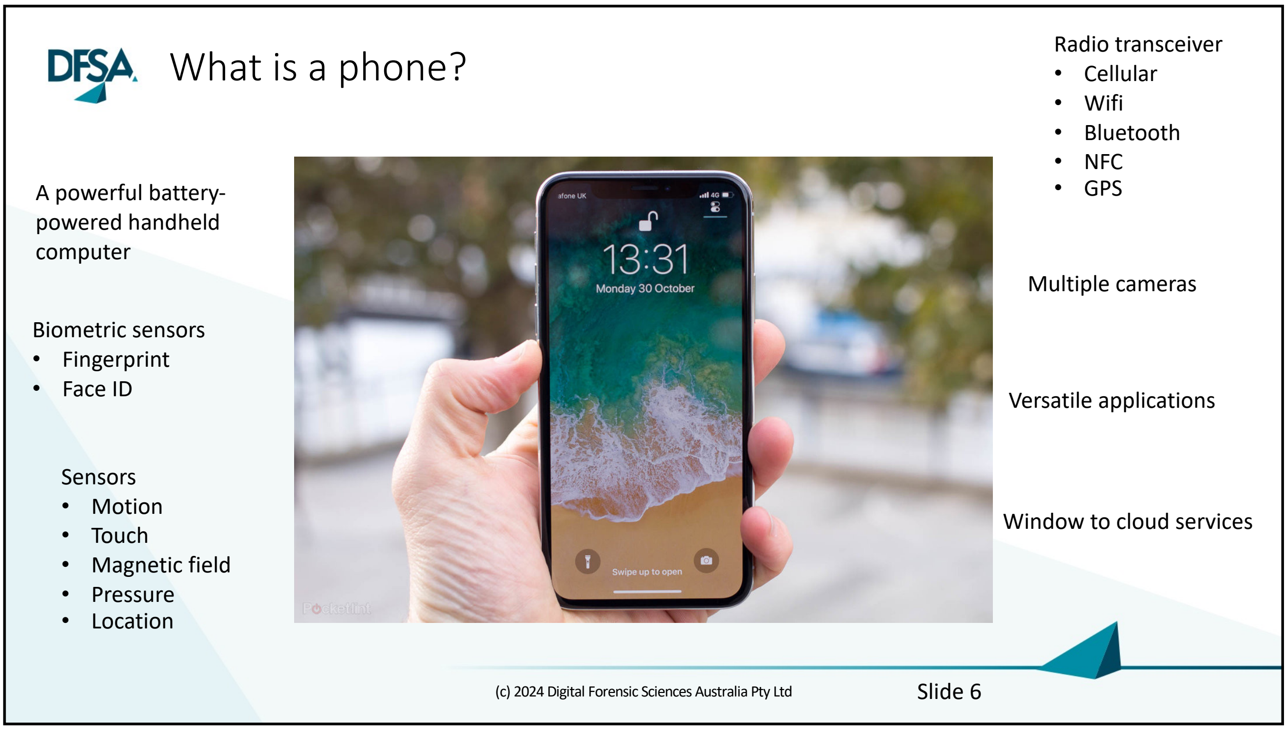
4



What is a phone?

Slide 5

5



What is a phone?

A powerful battery-powered handheld computer

Biometric sensors
- Fingerprint
- Face ID

Sensors
- Motion
- Touch
- Magnetic field
- Pressure
- Location

Radio transceiver
- Cellular
- Wifi
- Bluetooth
- NFC
- GPS

Multiple cameras

Versatile applications

Window to cloud services

Slide 6

6

What is a phone?

Banking

Transport/Uber

Identity/Certification

Calendar

Communications device

Casual hookup dating

Remote control / IoT

Navigation

Credit card

Calculator

Photo and video library

Social media platform

Streamed video player

Games

Gambling

Search at your fingertips

Tracker

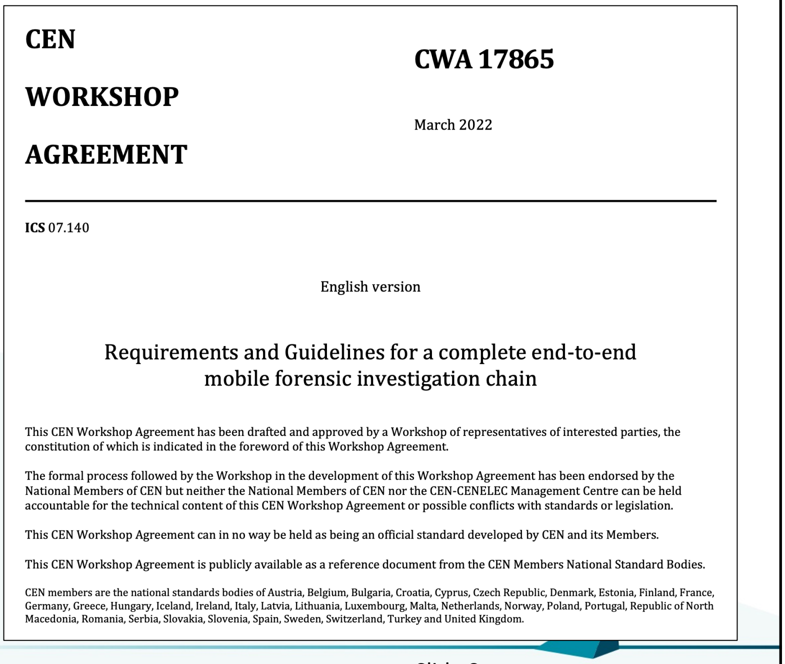
Health monitor

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

Slide 7

7

New European Standard



CEN

WORKSHOP

AGREEMENT

CWA 17865

March 2022

ICS 07.140

English version

Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

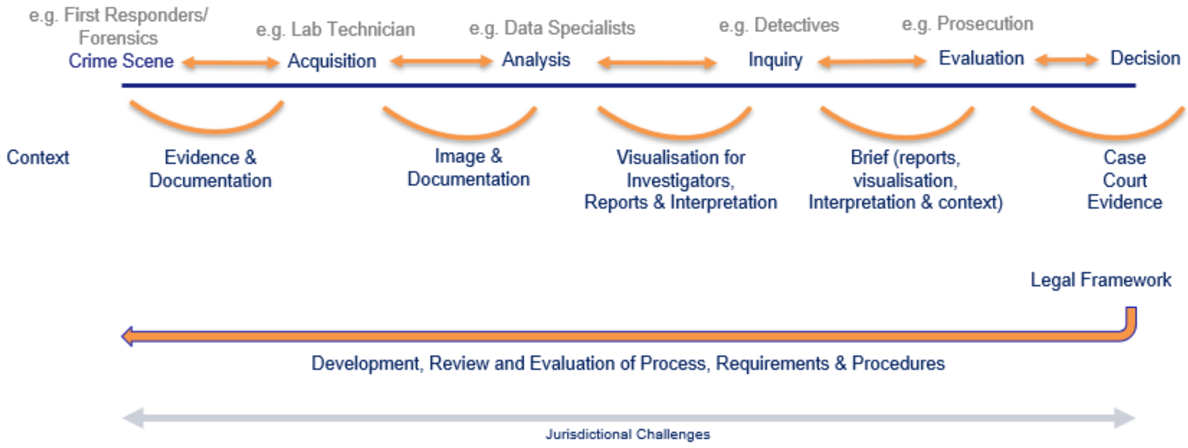
CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

Slide 8

8

Slide 9



e.g. First Responders/ Forensics

Crime Scene

e.g. Lab Technician

Acquisition

e.g. Data Specialists

Analysis

e.g. Detectives

Inquiry

e.g. Prosecution

Evaluation

Decision

Context

Evidence & Documentation

Image & Documentation

Visualisation for Investigators, Reports & Interpretation

Brief (reports, visualisation, Interpretation & context)

Case Court Evidence

Legal Framework

Development, Review and Evaluation of Process, Requirements & Procedures

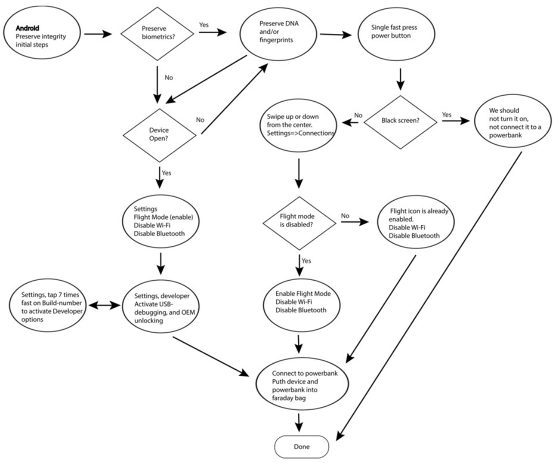
Jurisdictional Challenges

Law Enforcement educational challenges for mobile forensics, Humphries, Nordvik, Manifavas, Cobley & Sorell, Digital Investigation (accepted 2020)

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

9

Slide 10


Android
Preserve integrity initial steps
Preserve biometrics?
Yes
No
Preserve DNA and/or fingerprints
Single fast press power button
Device Open?
No
Yes
Black screen?
No
Yes
Swipe up or down from the center. Settings=>Connections
We should not turn it on, not connect it to a powerbank
Settings
Flight Mode (enable)
Disable Wi-Fi
Disable Bluetooth
Flight mode is disabled?
No
Yes
Flight icon is already enabled.
Disable Wi-Fi
Disable Bluetooth
Settings, tap 7 times fast on Build-number to activate Developer options
Settings, developer Activate USB-debugging, and OEM unlocking
Enable Flight Mode
Disable Wi-Fi
Disable Bluetooth
Connect to powerbank Puth device and powerbank into faraday bag
Done

Flowchart giving advise to the first responder

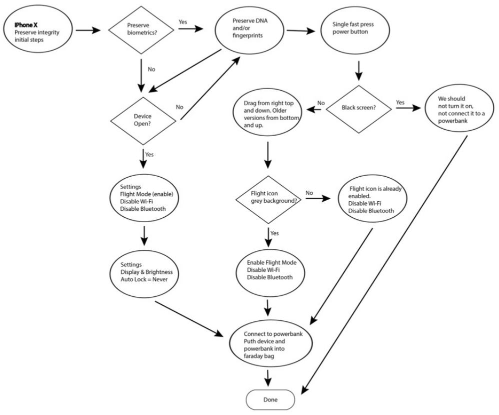
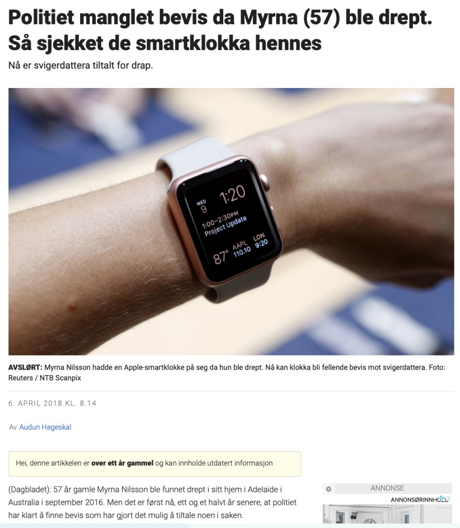

IPhone X
Preserve integrity initial steps
Preserve biometrics?
Yes
No
Preserve DNA and/or fingerprints
Single fast press power button
Device Open?
No
Yes
Black screen?
No
Yes
Drag from right top and down. Older versions from bottom and up.
We should not turn it on, not connect it to a powerbank
Settings
Flight Mode (enable)
Disable Wi-Fi
Disable Bluetooth
Flight icon grey background?
No
Yes
Flight icon is already enabled.
Disable Wi-Fi
Disable Bluetooth
Settings
Display & Brightness
Auto Lock = Never
Enable Flight Mode
Disable Wi-Fi
Disable Bluetooth
Connect to powerbank Puth device and powerbank into faraday bag
Done

Chart Diagram showing what to do with an iPhone X at the crime scene

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

10

Your digital aura



Politiet manglet bevis da Myrna (57) ble drept. Så sjekket de smartklokka hennes

Nå er svigerdattera tiltalt for drap.

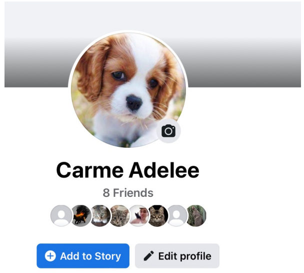
AVSLØRT: Myrna Nilsson hadde en Apple-smartklokke på seg da hun ble drept. Nå kan klokka bli fellende bevis mot svigerdattera. Foto: Reuters / NTB Scanpix

6. APRIL 2018 KL. 8.14

Av Audun Hageskal

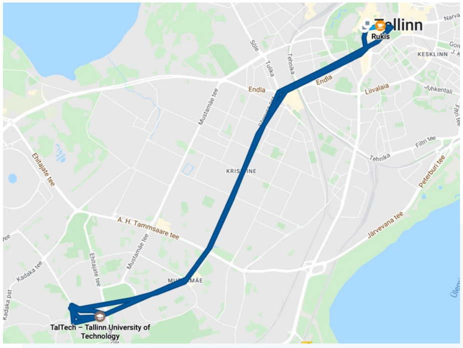
Hei, denne artikkelen er **over ett år gammel** og kan innholde utdatert informasjon

(Dagbladet): 57 år gamle Myrna Nilsson ble funnet drept i sitt hjem i Adelaide i Australia i september 2016. Men det er først nå, ett og et halvt år senere, at politiet har klart å finne bevis som har gjort det mulig å tiltale noen i saken.



Carme Adelee

8 Friends



Pornhub

Commonwealth Bank

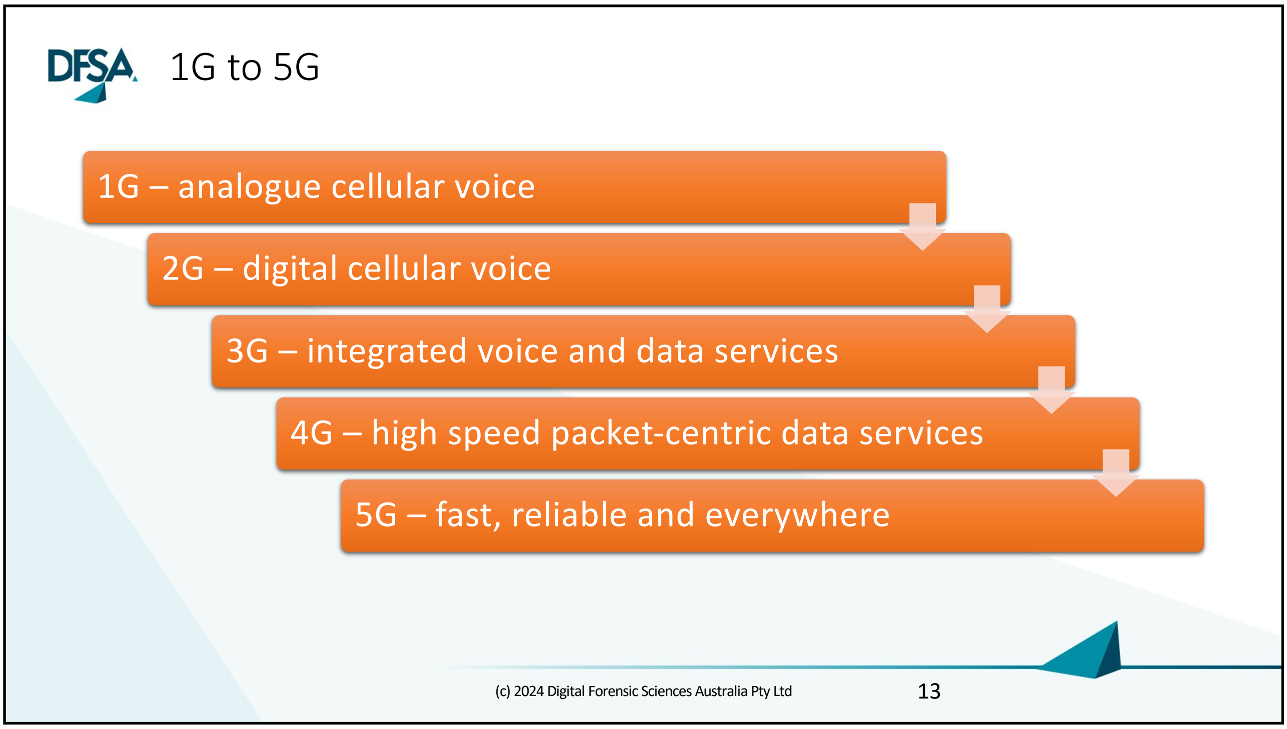
Google

11

ELEC ENG 7080
Module 1: Introduction
1G to 5G

Mobile Phone Forensics

12

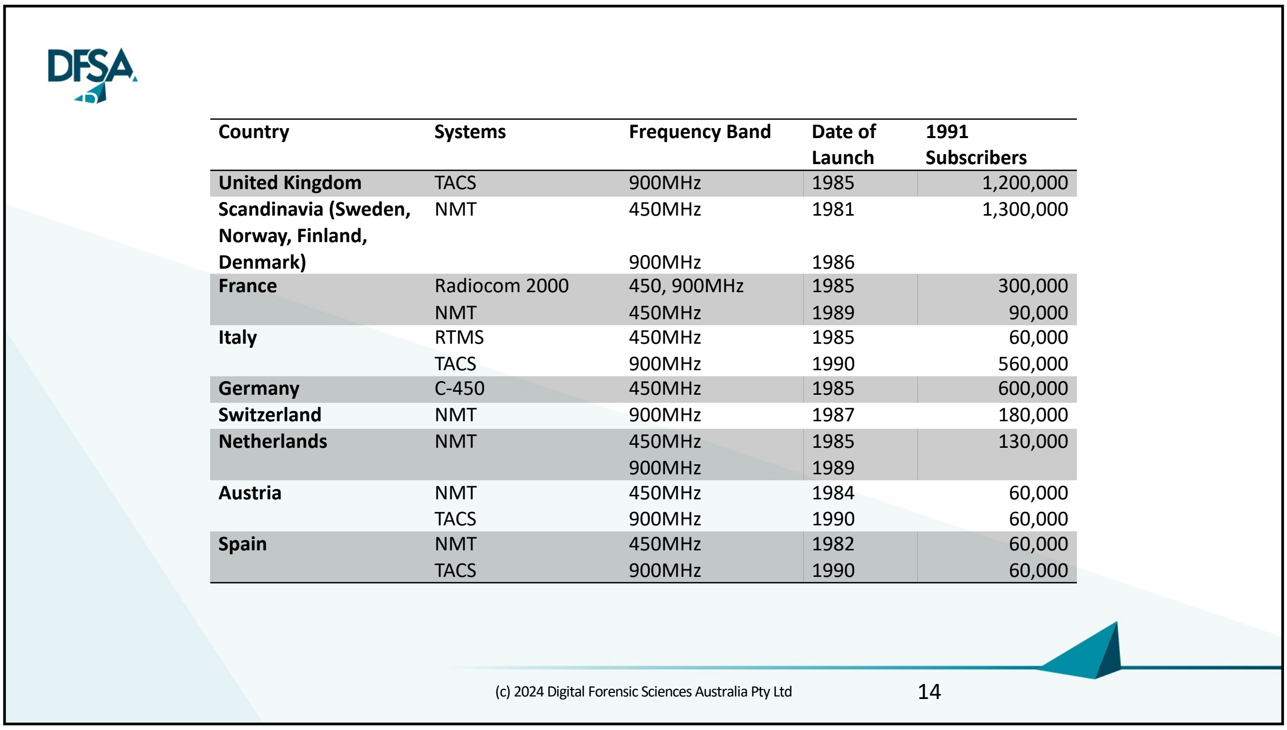


1G to 5G

- 1G – analogue cellular voice
- 2G – digital cellular voice
- 3G – integrated voice and data services
- 4G – high speed packet-centric data services
- 5G – fast, reliable and everywhere

(c) 2024 Digital Forensic Sciences Australia Pty Ltd 13

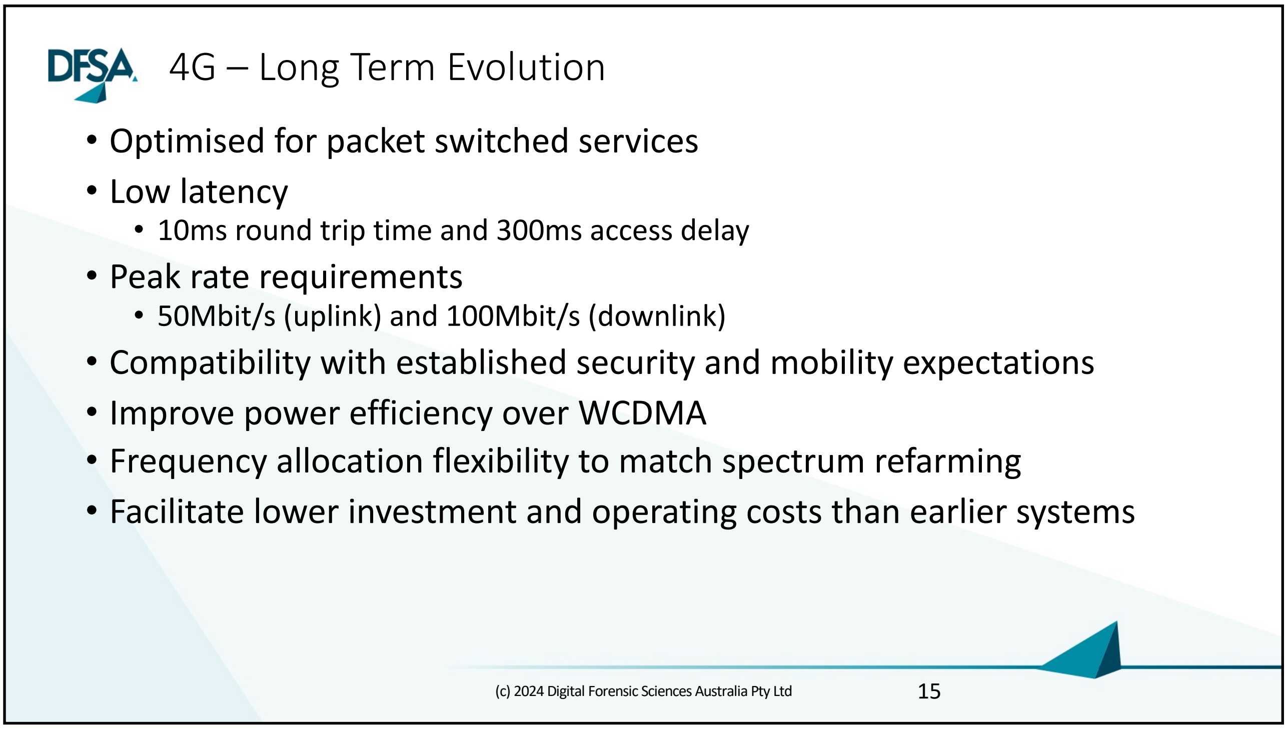
13



Country	Systems	Frequency Band	Date of Launch	1991 Subscribers
United Kingdom	TACS	900MHz	1985	1,200,000
Scandinavia (Sweden, Norway, Finland, Denmark)	NMT	450MHz 900MHz	1981 1986	1,300,000
France	Radiocom 2000	450, 900MHz	1985	300,000
	NMT	450MHz	1989	90,000
Italy	RTMS	450MHz	1985	60,000
	TACS	900MHz	1990	560,000
Germany	C-450	450MHz	1985	600,000
Switzerland	NMT	900MHz	1987	180,000
Netherlands	NMT	450MHz 900MHz	1985 1989	130,000
Austria	NMT	450MHz	1984	60,000
	TACS	900MHz	1990	60,000
Spain	NMT	450MHz	1982	60,000
	TACS	900MHz	1990	60,000

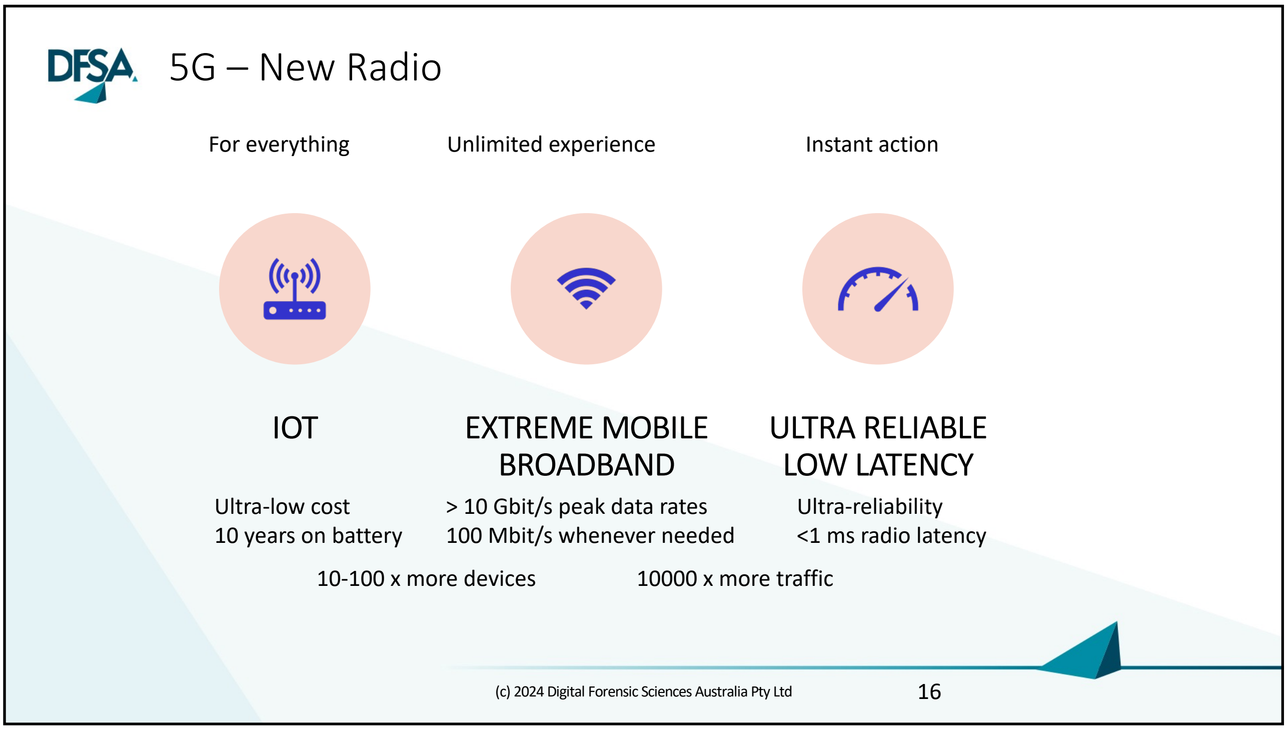
(c) 2024 Digital Forensic Sciences Australia Pty Ltd 14

14



4G – Long Term Evolution

- Optimised for packet switched services
- Low latency
  - 10ms round trip time and 300ms access delay
- Peak rate requirements
  - 50Mbit/s (uplink) and 100Mbit/s (downlink)
- Compatibility with established security and mobility expectations
- Improve power efficiency over WCDMA
- Frequency allocation flexibility to match spectrum refarming
- Facilitate lower investment and operating costs than earlier systems

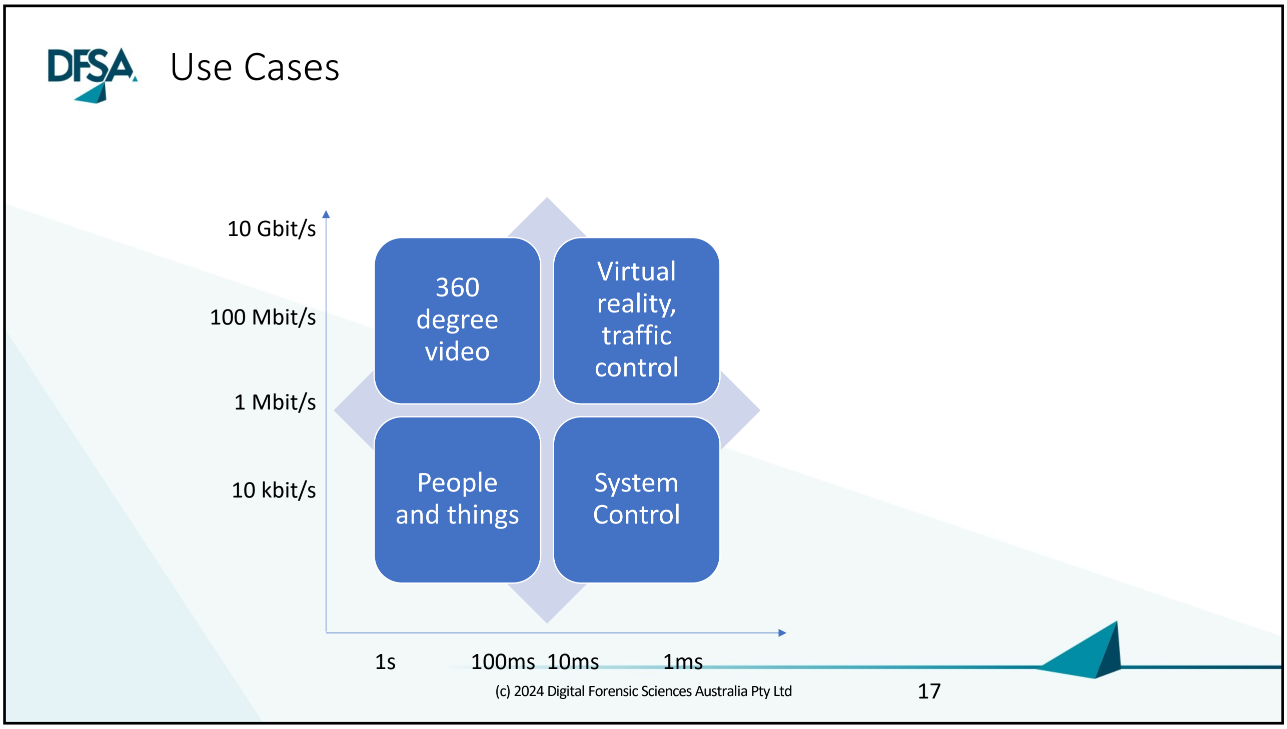


5G – New Radio

For everything	Unlimited experience	Instant action
IOT	EXTREME MOBILE BROADBAND	ULTRA RELIABLE LOW LATENCY
Ultra-low cost 10 years on battery	> 10 Gbit/s peak data rates 100 Mbit/s whenever needed	Ultra-reliability <1 ms radio latency

10-100 x more devices

10000 x more traffic



Use Cases

10 Gbit/s

100 Mbit/s

1 Mbit/s

10 kbit/s

360 degree video

Virtual reality, traffic control

People and things

System Control

1s 100ms 10ms 1ms

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

17

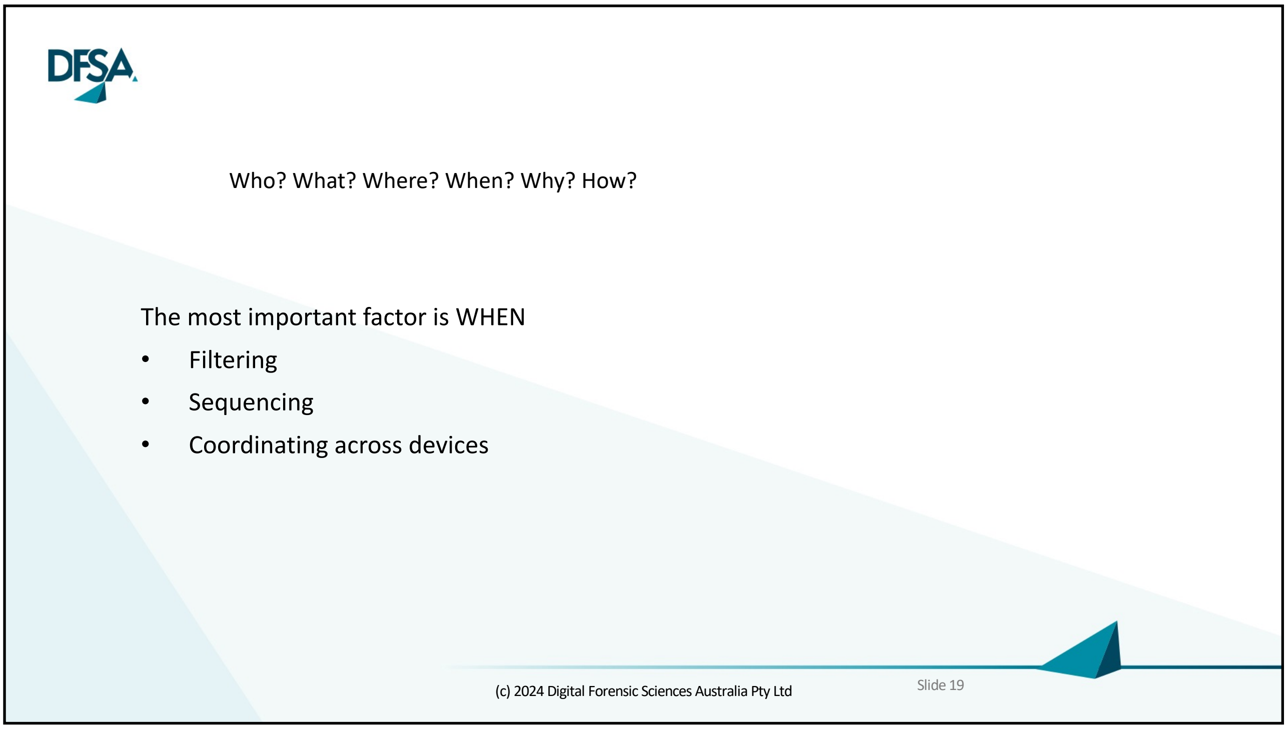
17

It’s about time

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

18

18

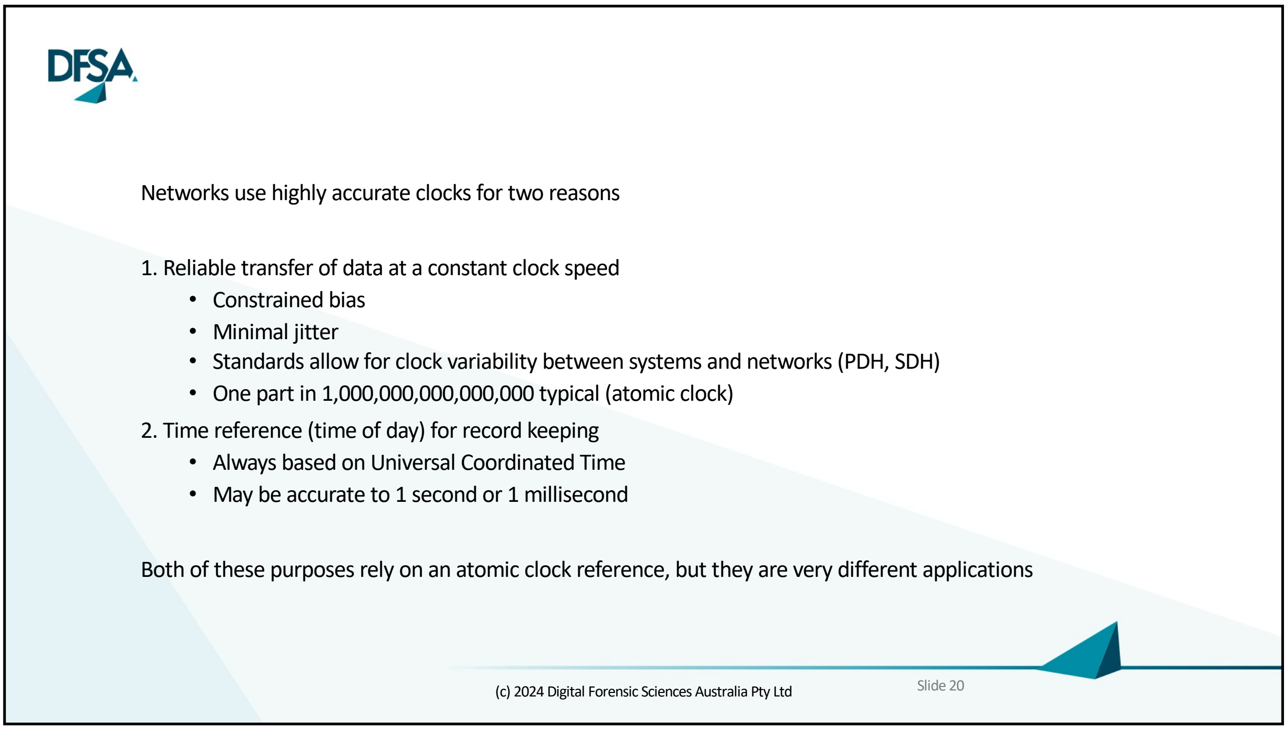


Who? What? Where? When? Why? How?

The most important factor is WHEN

- Filtering
- Sequencing
- Coordinating across devices

19



Networks use highly accurate clocks for two reasons

1. Reliable transfer of data at a constant clock speed
   - Constrained bias
   - Minimal jitter
   - Standards allow for clock variability between systems and networks (PDH, SDH)
   - One part in 1,000,000,000,000,000 typical (atomic clock)
2. Time reference (time of day) for record keeping
   - Always based on Universal Coordinated Time
   - May be accurate to 1 second or 1 millisecond

Both of these purposes rely on an atomic clock reference, but they are very different applications

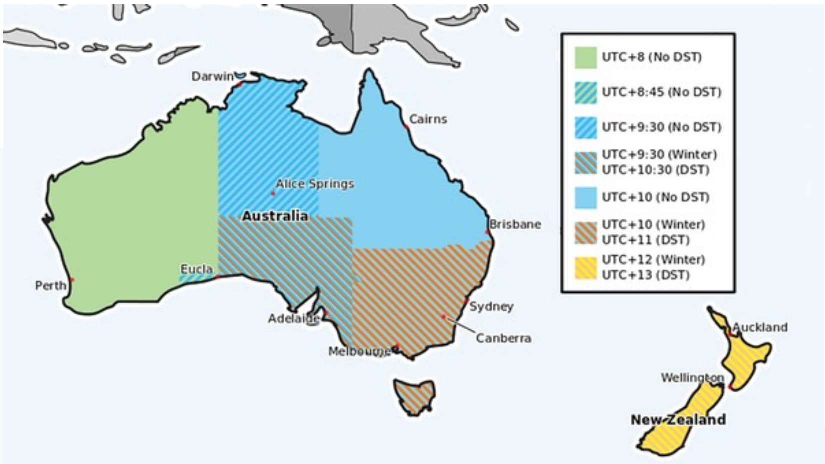
20

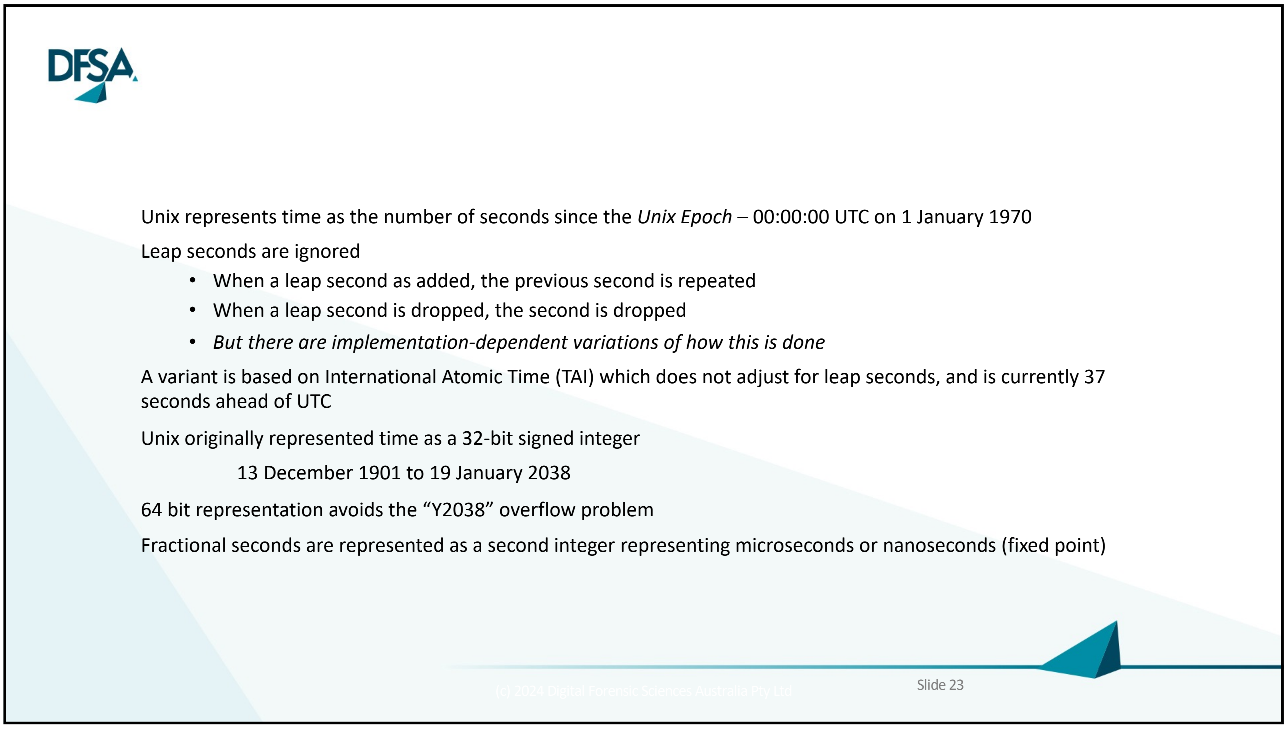
Universal Time 1 (UT1)

- Conceptually, mean solar time at 0 degrees longitude
- In practice, determined using astronomical observations of distant quasars, the Moon, artificial satellites etc

Universal Coordinated Time is *based on* UT1

- 86400 SI seconds per day, kept within 0.9 seconds of UT1 by occasional leap seconds
- Other equivalent terms are "Greenwich Mean Time" and "Zulu Time"





DFSA

Unix represents time as the number of seconds since the *Unix Epoch* – 00:00:00 UTC on 1 January 1970

Leap seconds are ignored

- When a leap second as added, the previous second is repeated
- When a leap second is dropped, the second is dropped
- *But there are implementation-dependent variations of how this is done*

A variant is based on International Atomic Time (TAI) which does not adjust for leap seconds, and is currently 37 seconds ahead of UTC

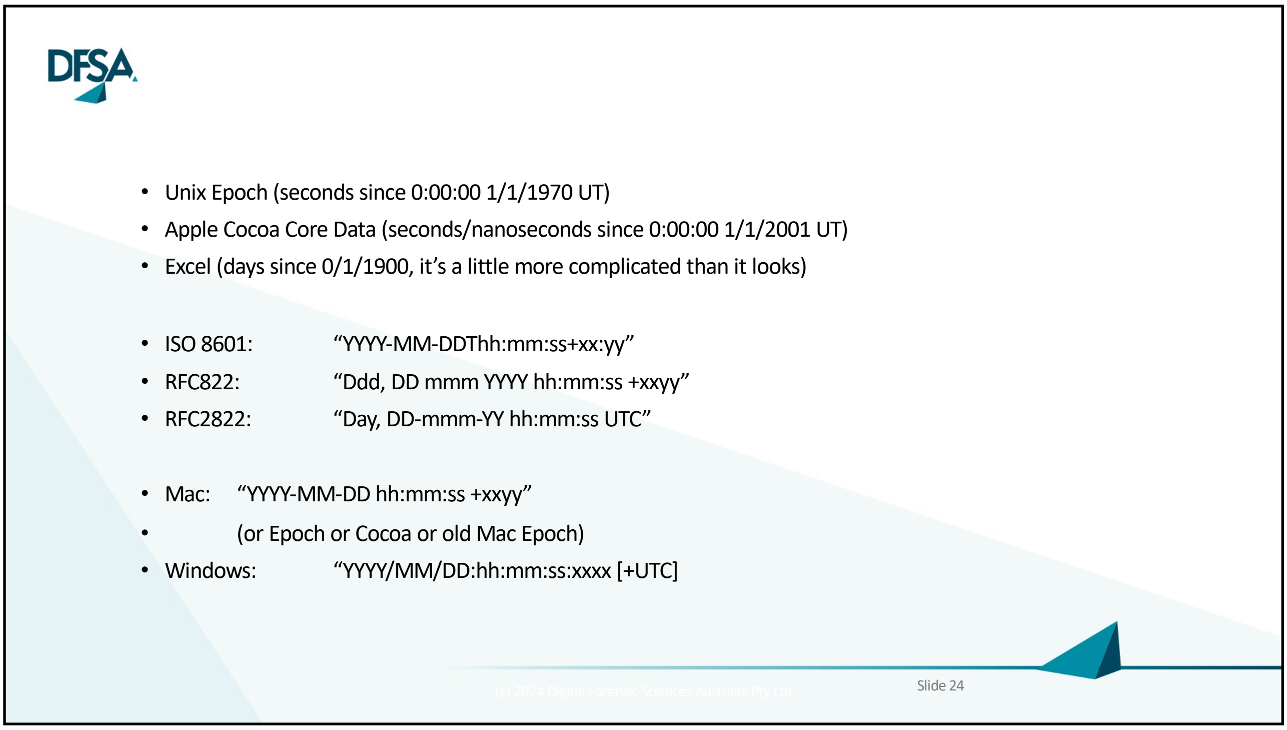
Unix originally represented time as a 32-bit signed integer

13 December 1901 to 19 January 2038

64 bit representation avoids the "Y2038" overflow problem

Fractional seconds are represented as a second integer representing microseconds or nanoseconds (fixed point)

23



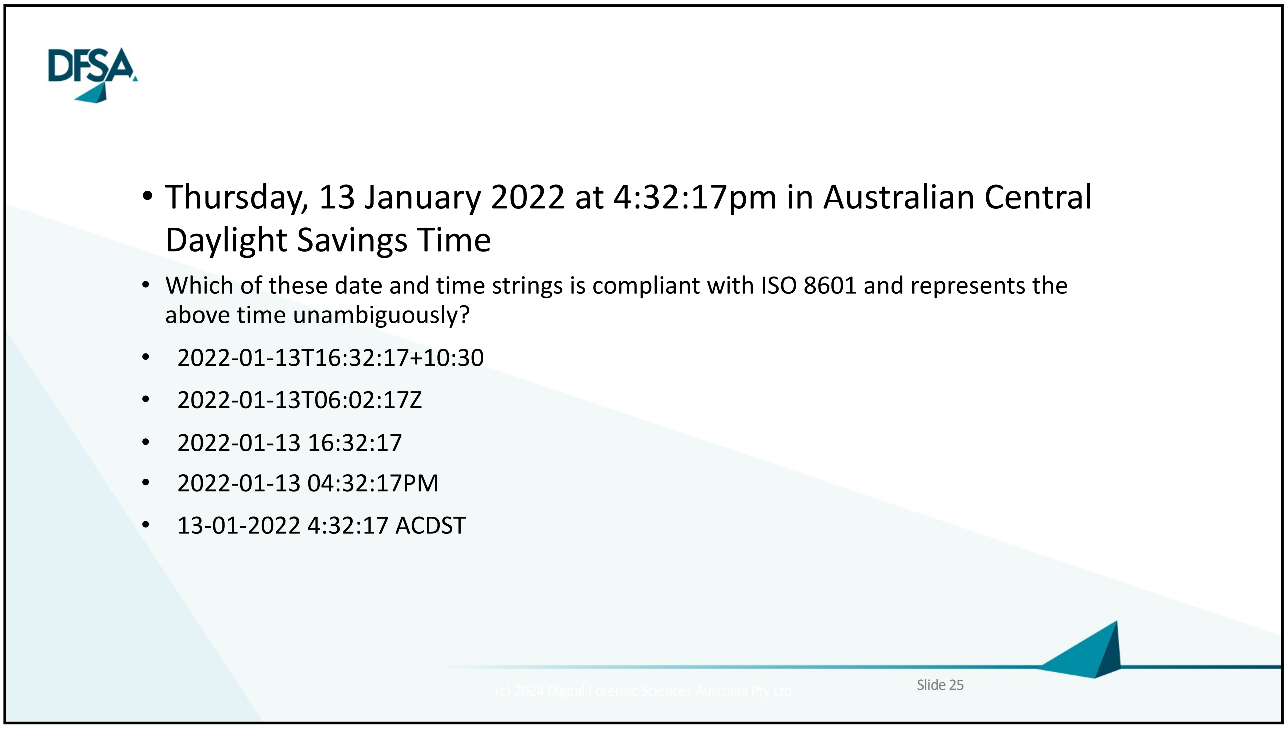
DFSA

- Unix Epoch (seconds since 0:00:00 1/1/1970 UT)
- Apple Cocoa Core Data (seconds/nanoseconds since 0:00:00 1/1/2001 UT)
- Excel (days since 0/1/1900, it's a little more complicated than it looks)

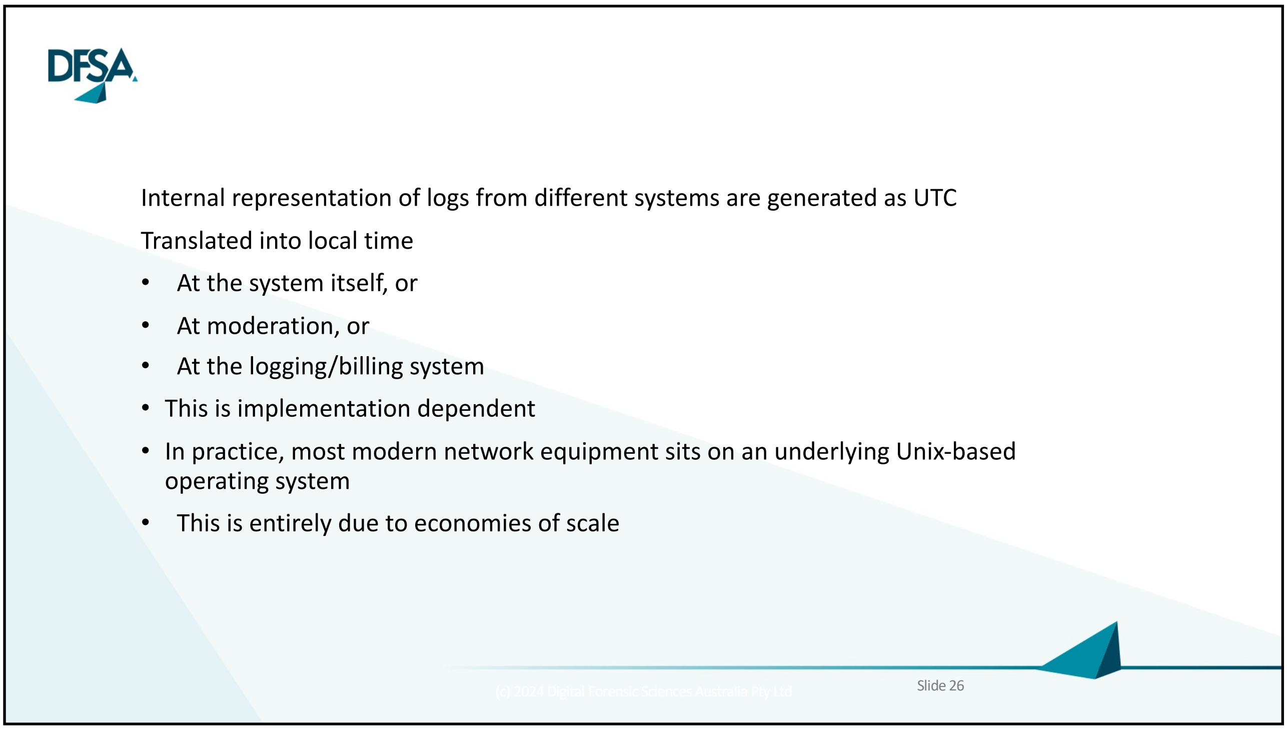
- ISO 8601: "YYYY-MM-DDThh:mm:ss+xx:yy"
- RFC822: "Ddd, DD mmm YYYY hh:mm:ss +xxyy"
- RFC2822: "Day, DD-mmm-YY hh:mm:ss UTC"

- Mac: "YYYY-MM-DD hh:mm:ss +xxyy"
- (or Epoch or Cocoa or old Mac Epoch)
- Windows: "YYYY/MM/DD:hh:mm:ss:xxxx [+UTC]

24



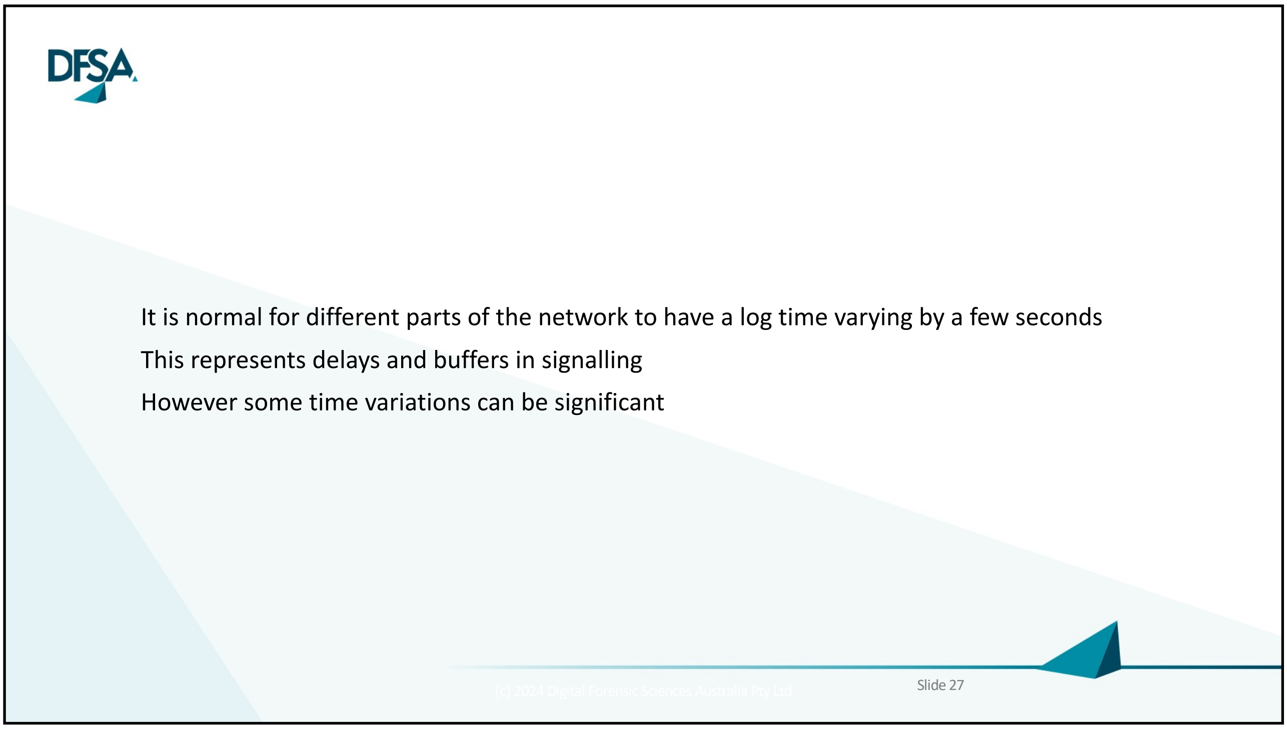
- Thursday, 13 January 2022 at 4:32:17pm in Australian Central Daylight Savings Time
- Which of these date and time strings is compliant with ISO 8601 and represents the above time unambiguously?
- 2022-01-13T16:32:17+10:30
- 2022-01-13T06:02:17Z
- 2022-01-13 16:32:17
- 2022-01-13 04:32:17PM
- 13-01-2022 4:32:17 ACDST



Internal representation of logs from different systems are generated as UTC

Translated into local time

- At the system itself, or
- At moderation, or
- At the logging/billing system
- This is implementation dependent
- In practice, most modern network equipment sits on an underlying Unix-based operating system
- This is entirely due to economies of scale



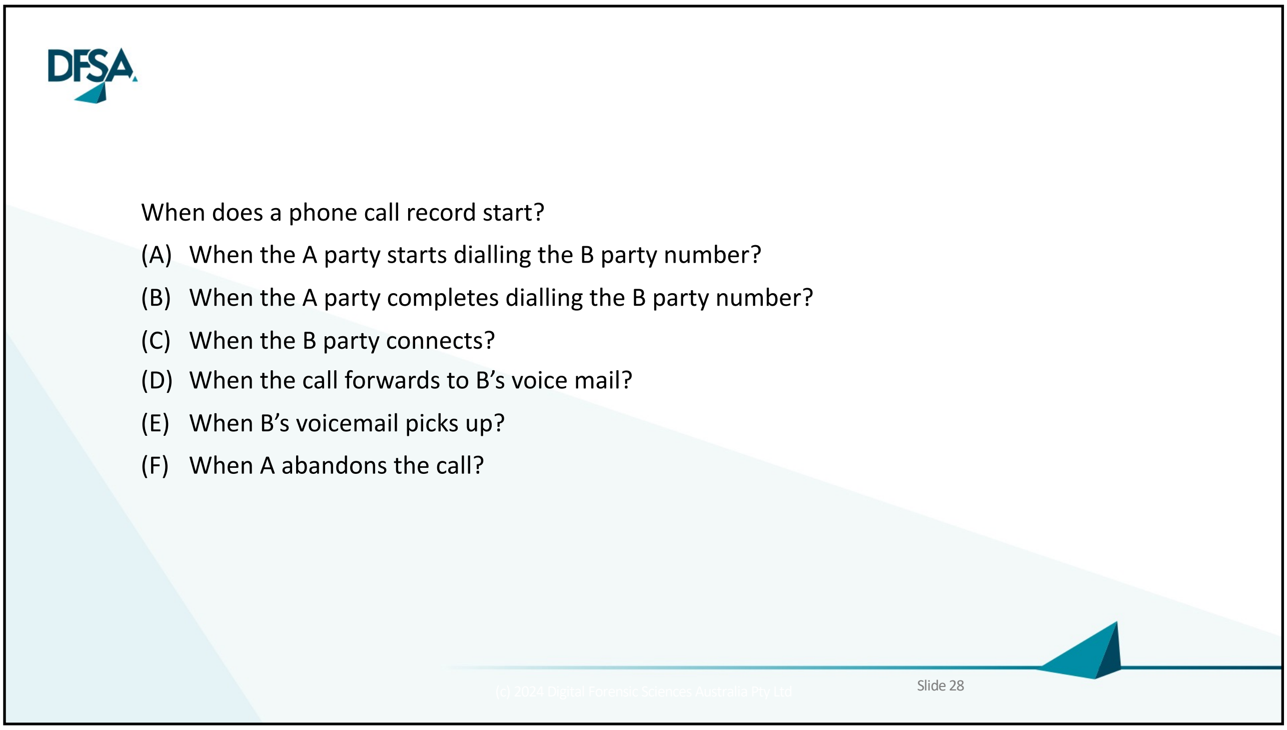
It is normal for different parts of the network to have a log time varying by a few seconds

This represents delays and buffers in signalling

However some time variations can be significant

Slide 27

27



When does a phone call record start?

(A) When the A party starts dialling the B party number?

(B) When the A party completes dialling the B party number?

(C) When the B party connects?

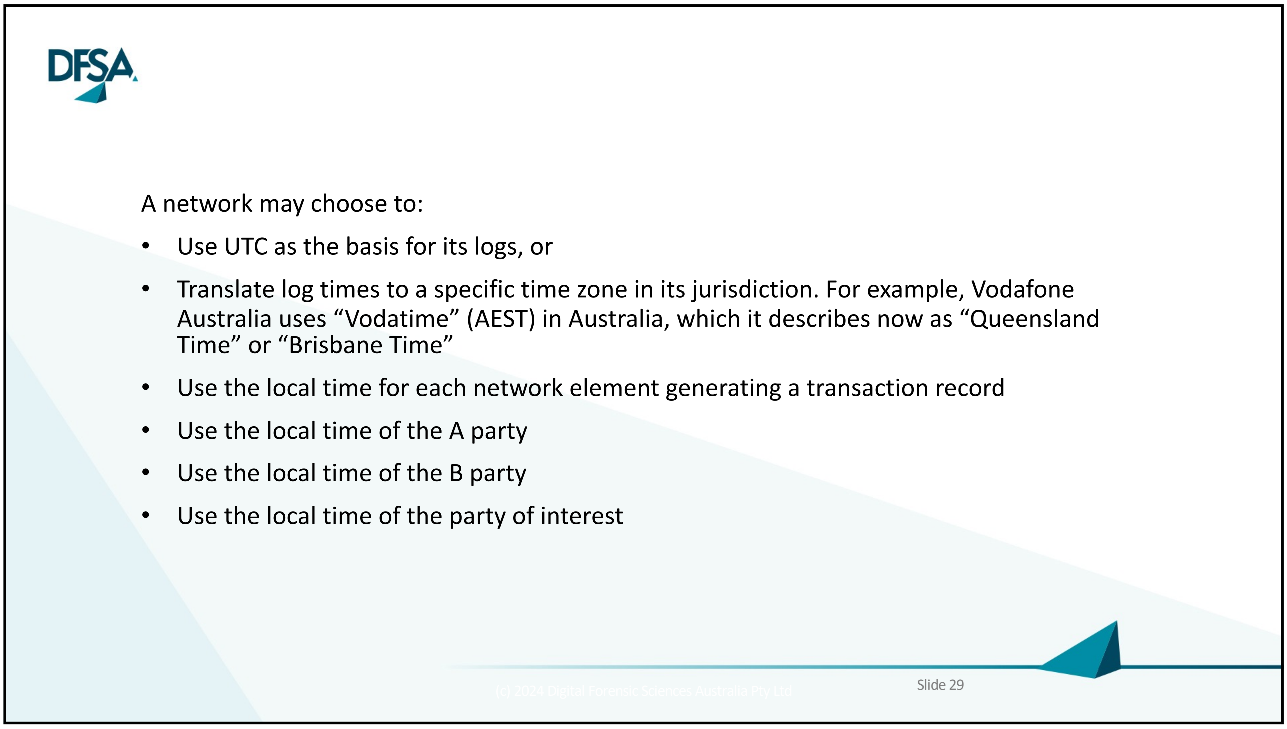
(D) When the call forwards to B’s voice mail?

(E) When B’s voicemail picks up?

(F) When A abandons the call?

Slide 28

28

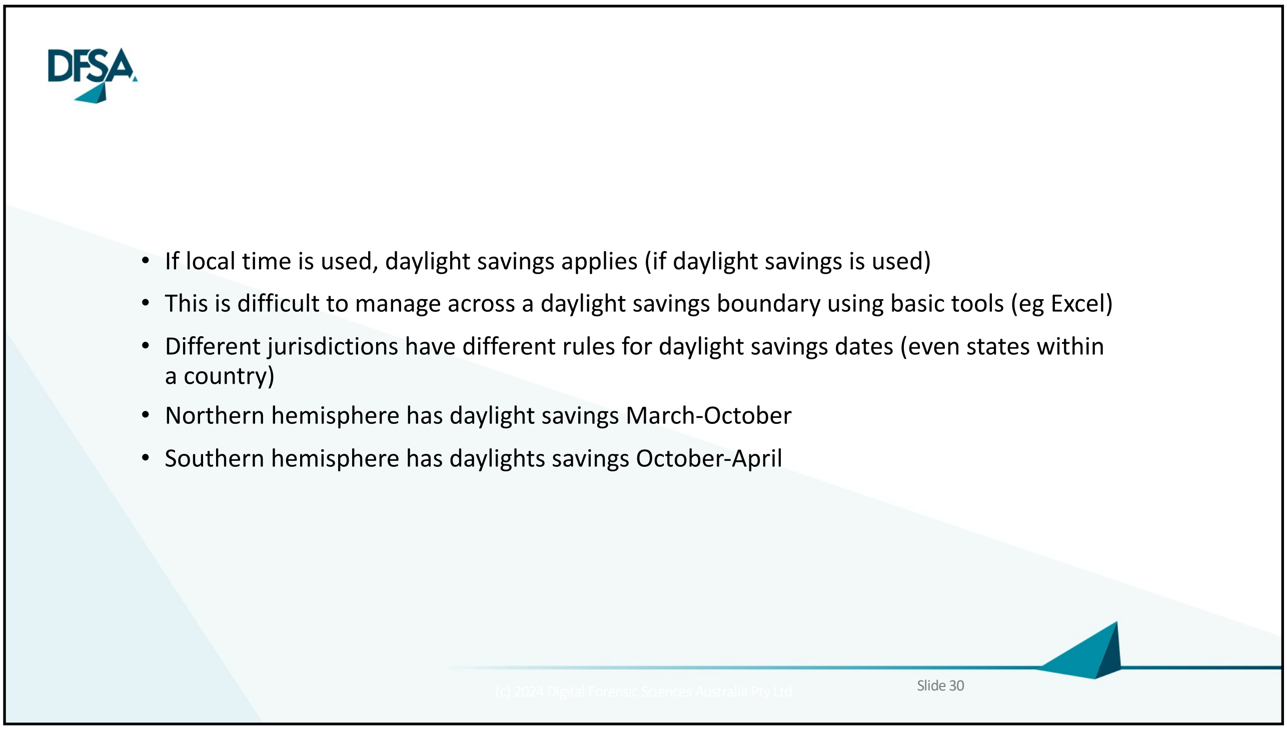


A network may choose to:

- Use UTC as the basis for its logs, or
- Translate log times to a specific time zone in its jurisdiction. For example, Vodafone Australia uses “Vodatime” (AEST) in Australia, which it describes now as “Queensland Time” or “Brisbane Time”
- Use the local time for each network element generating a transaction record
- Use the local time of the A party
- Use the local time of the B party
- Use the local time of the party of interest

Slide 29

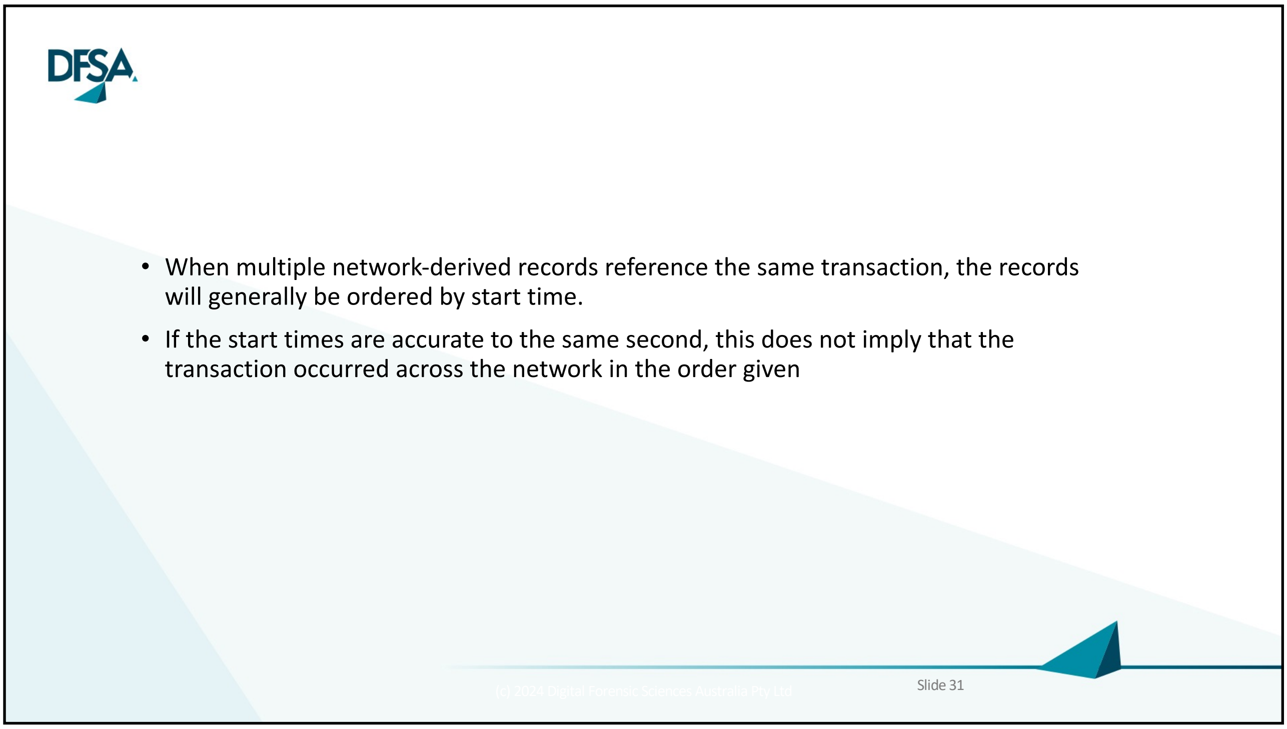
29



- If local time is used, daylight savings applies (if daylight savings is used)
- This is difficult to manage across a daylight savings boundary using basic tools (eg Excel)
- Different jurisdictions have different rules for daylight savings dates (even states within a country)
- Northern hemisphere has daylight savings March-October
- Southern hemisphere has daylights savings October-April

Slide 30

30



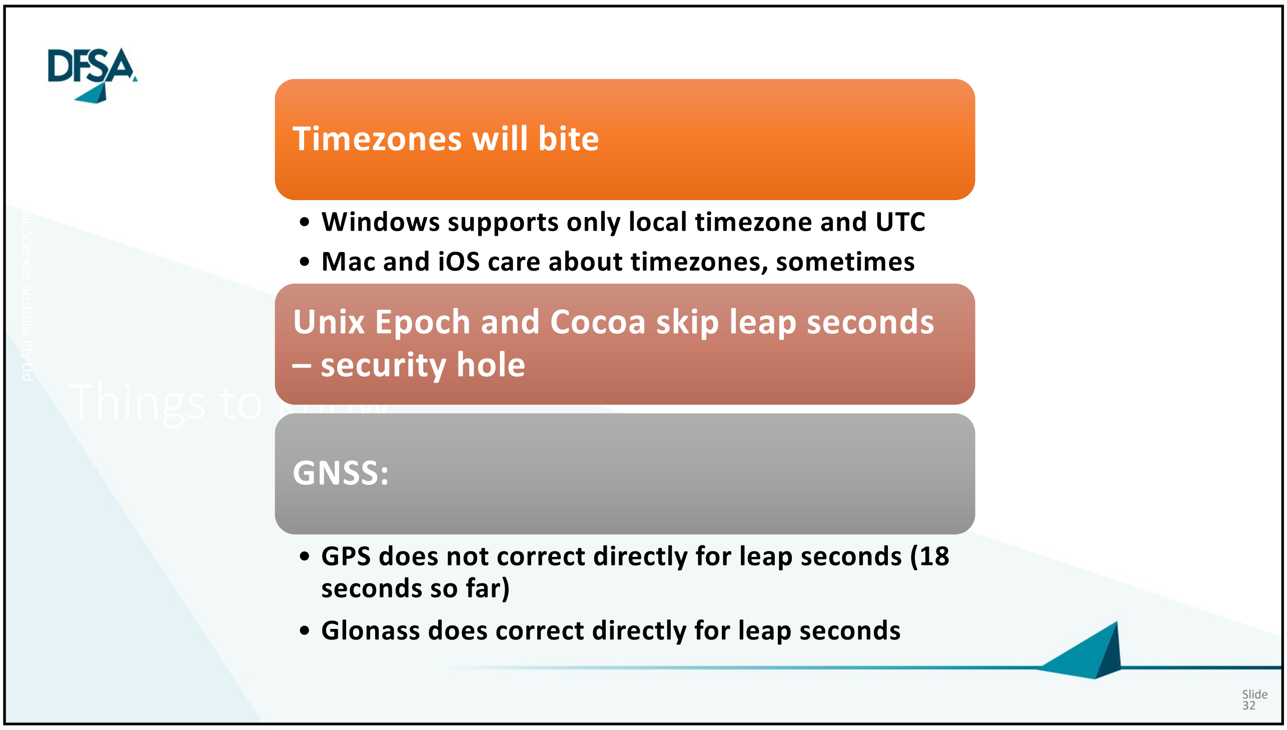
DFSA

- When multiple network-derived records reference the same transaction, the records will generally be ordered by start time.
- If the start times are accurate to the same second, this does not imply that the transaction occurred across the network in the order given

(c) 2024 Digital Forensic Sciences Australia Pty Ltd

Slide 31

31



DFSA

Things to know

Timezones will bite

- **Windows supports only local timezone and UTC**
- **Mac and iOS care about timezones, sometimes**

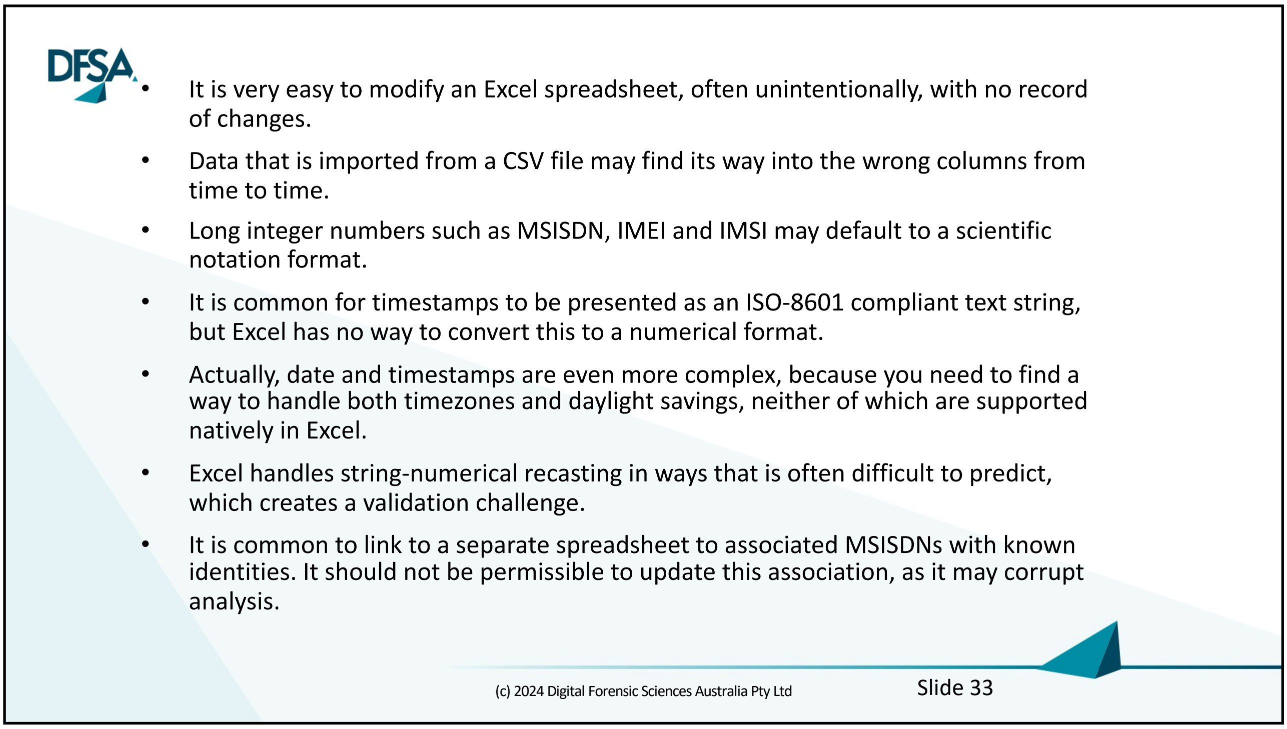
Unix Epoch and Cocoa skip leap seconds – security hole

GNSS:

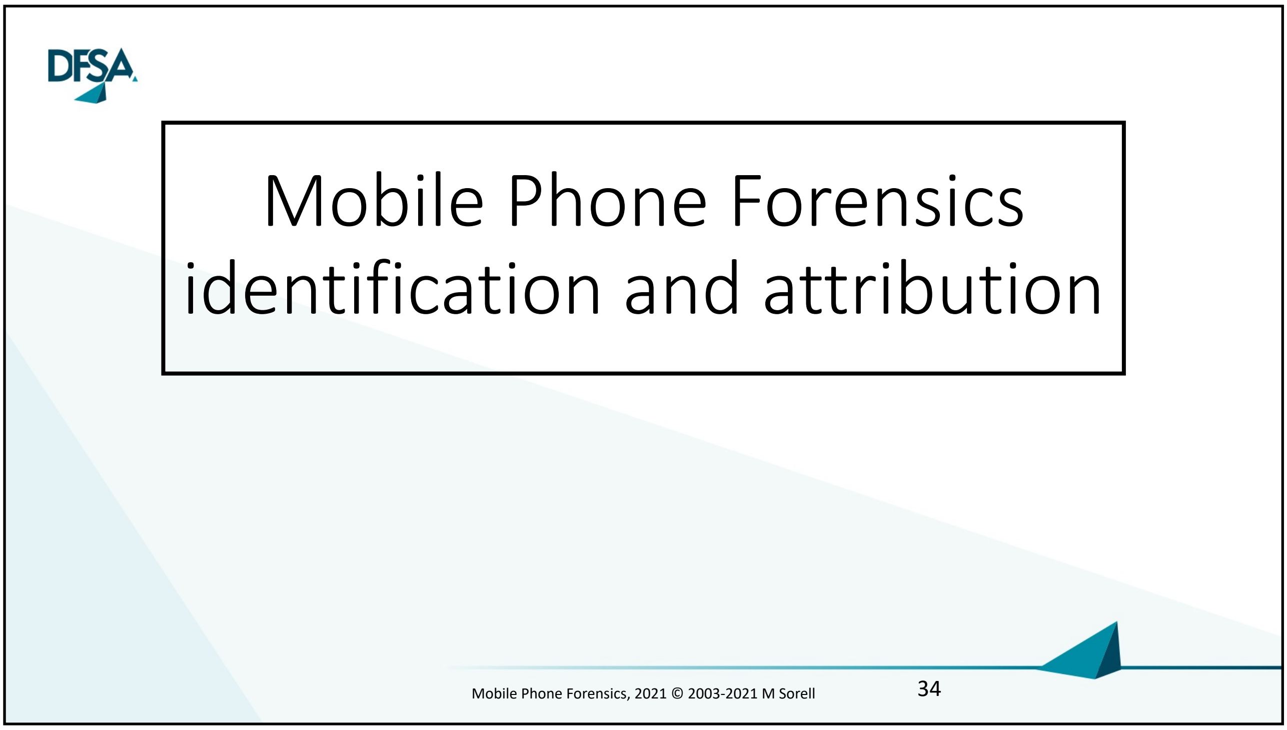
- **GPS does not correct directly for leap seconds (18 seconds so far)**
- **Glonass does correct directly for leap seconds**

Slide 32

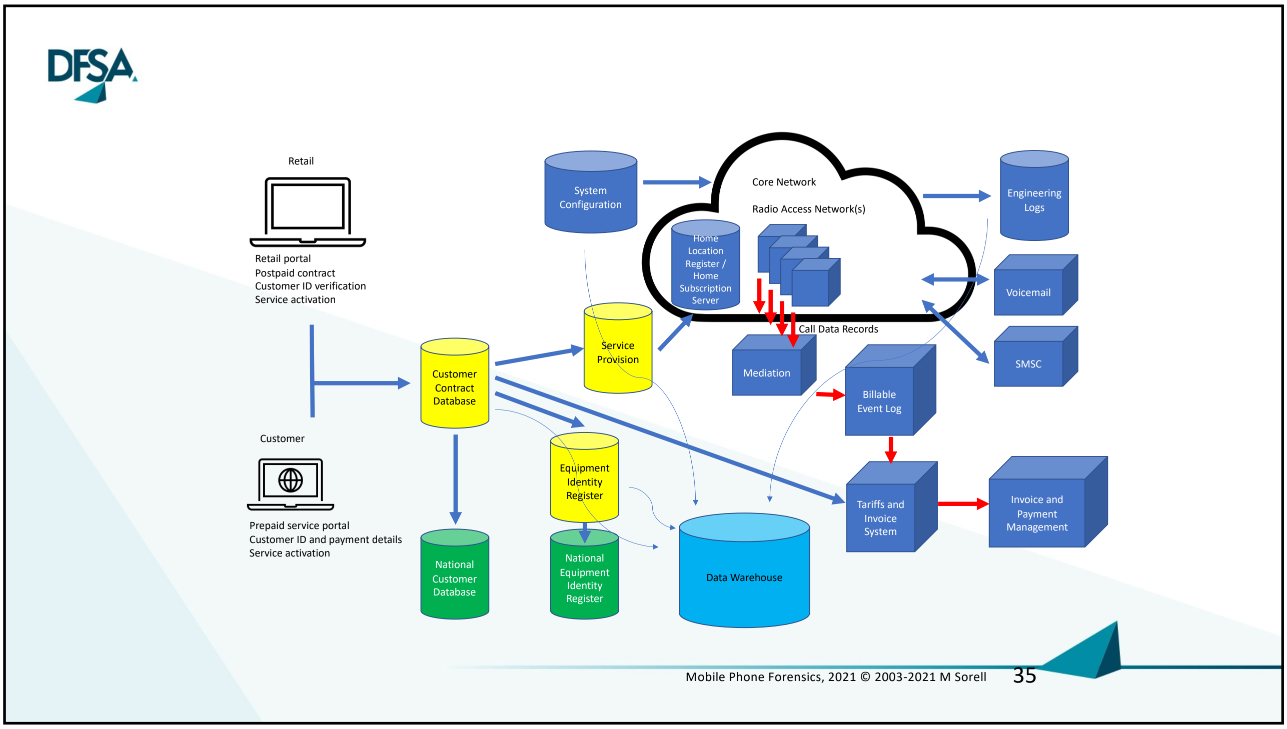
32

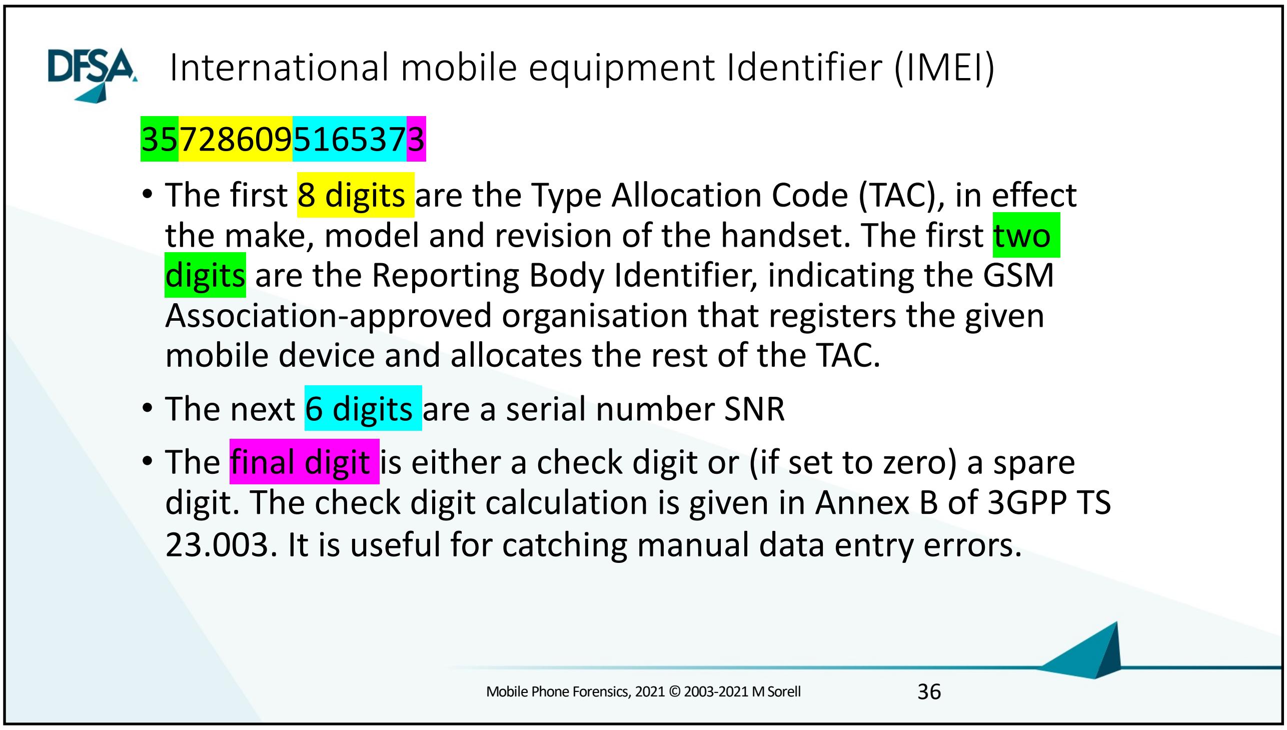


- It is very easy to modify an Excel spreadsheet, often unintentionally, with no record of changes.
- Data that is imported from a CSV file may find its way into the wrong columns from time to time.
- Long integer numbers such as MSISDN, IMEI and IMSI may default to a scientific notation format.
- It is common for timestamps to be presented as an ISO-8601 compliant text string, but Excel has no way to convert this to a numerical format.
- Actually, date and timestamps are even more complex, because you need to find a way to handle both timezones and daylight savings, neither of which are supported natively in Excel.
- Excel handles string-numerical recasting in ways that is often difficult to predict, which creates a validation challenge.
- It is common to link to a separate spreadsheet to associated MSISDNs with known identities. It should not be permissible to update this association, as it may corrupt analysis.



Mobile Phone Forensics identification and attribution



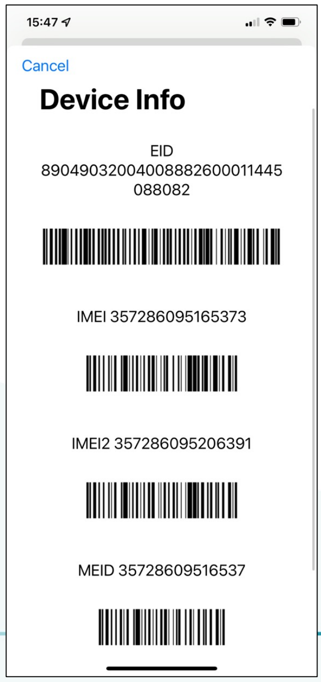


International mobile equipment Identifier (IMEI)

357286095165373

- The first 8 digits are the Type Allocation Code (TAC), in effect the make, model and revision of the handset. The first two digits are the Reporting Body Identifier, indicating the GSM Association-approved organisation that registers the given mobile device and allocates the rest of the TAC.
- The next 6 digits are a serial number SNR
- The final digit is either a check digit or (if set to zero) a spare digit. The check digit calculation is given in Annex B of 3GPP TS 23.003. It is useful for catching manual data entry errors.

Iphone *#06#



15:47

Cancel

Device Info

EID
89049032004008882600011445
088082

IMEI 357286095165373

IMEI2 357286095206391

MEID 35728609516537

37

INTERNATIONAL MOBILE SUBSCRIPTION IDENTIFIER

- The IMSI is up to 15 decimal digits, containing:
- Mobile Country Code (MCC) – 3 digits
- Mobile Network Code (MNC) – 2 or 3 digits
- Mobile Subscriber Identity Number (MSIN) – 8 to 10 digits

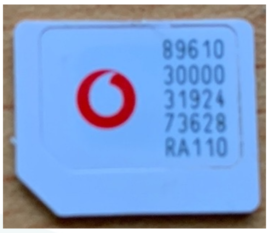
Example

505013141592653

38

Integrated circuit card identifier (ICCID)

- The first two digits are always 89 for a mobile SIM card, since the underlying card technology has other applications such as credit cards.
- The next two digits are the Country Code, in this case 61 (Australia). The country code is not the same as the MCC used in the IMSI.
- The next two digits is the Issue Identifier (03), which identifies the issuing home network, in this case Vodafone.
- The next 12 digits are the unique Account ID or serial number, in this case 0000 3192 4736.
- The final two digits (2) and (8) in this case are a checksum and an additional digit.



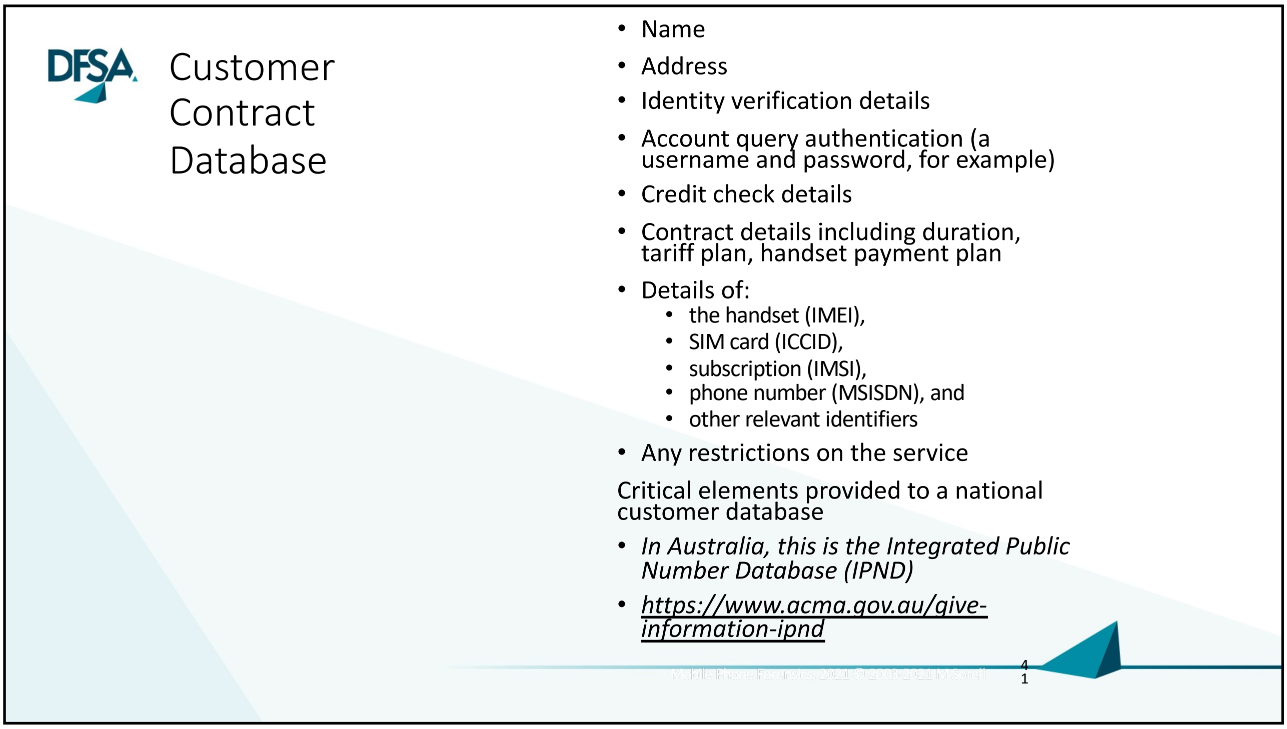
Mobile subscriber – integrated services digital network (MSISDN)

- A telephone number which follows the recommendations of the E.164 international standard "The international public telecommunications numbering plan"
- The MSISDN consists of a country code (1 to 3 digits) followed by a subscriber number of up to 12 digits. The subscriber number usually consists of a National Destination Code which is allocated to each in-country mobile network, followed by a unique subscriber number.

Examples

372 5877 6783

61 410 432 762



Customer Contract Database

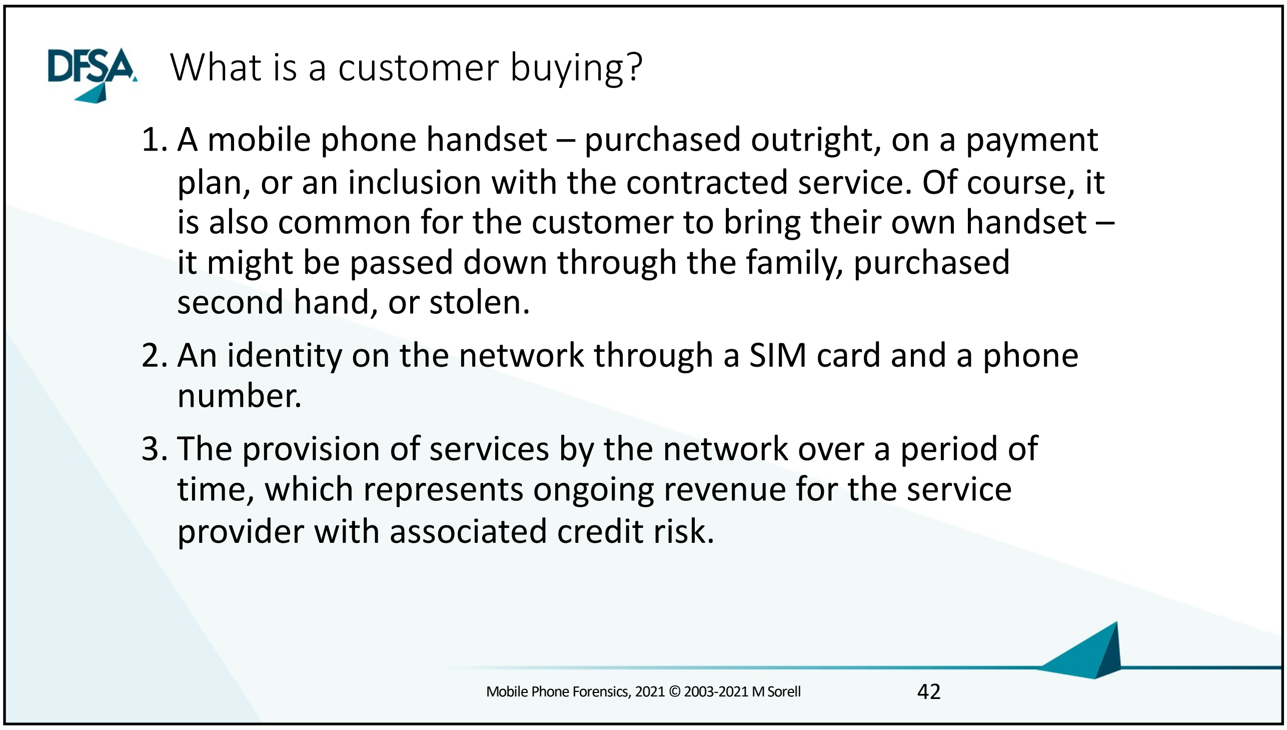
- Name
- Address
- Identity verification details
- Account query authentication (a username and password, for example)
- Credit check details
- Contract details including duration, tariff plan, handset payment plan
- Details of:
  - the handset (IMEI),
  - SIM card (ICCID),
  - subscription (IMSI),
  - phone number (MSISDN), and
  - other relevant identifiers
- Any restrictions on the service

Critical elements provided to a national customer database

- *In Australia, this is the Integrated Public Number Database (IPND)*
- *https://www.acma.gov.au/give-information-ipnd*

Mobile Phone Forensics, 2021 © 2003-2021 M Sorell 41

41

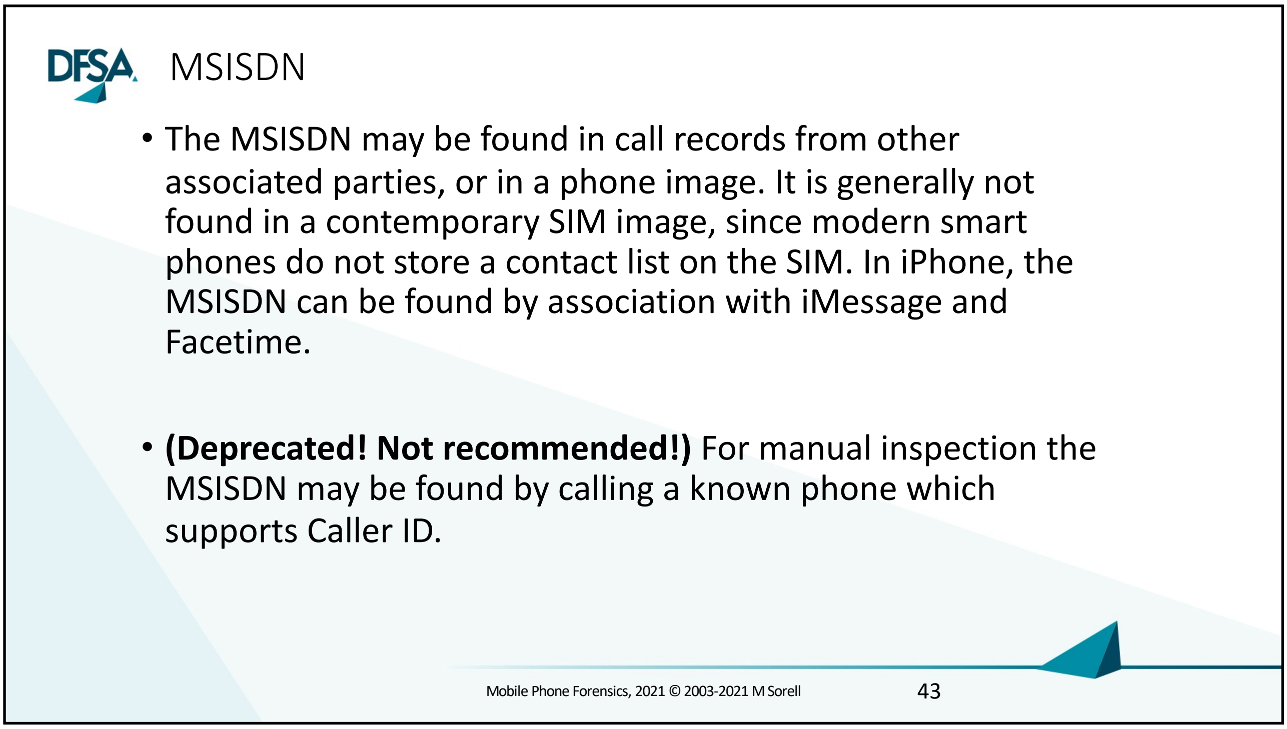


What is a customer buying?

1. A mobile phone handset – purchased outright, on a payment plan, or an inclusion with the contracted service. Of course, it is also common for the customer to bring their own handset – it might be passed down through the family, purchased second hand, or stolen.
2. An identity on the network through a SIM card and a phone number.
3. The provision of services by the network over a period of time, which represents ongoing revenue for the service provider with associated credit risk.

Mobile Phone Forensics, 2021 © 2003-2021 M Sorell 42

42

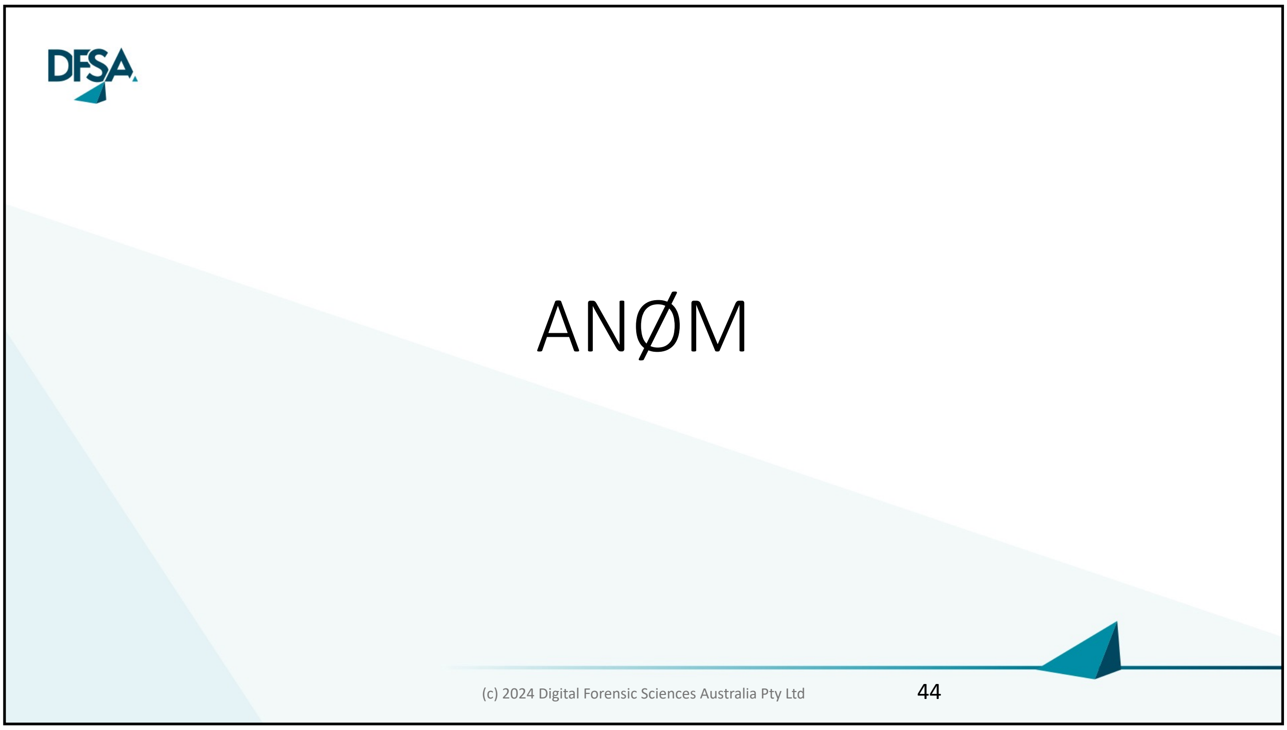


MSISDN

- The MSISDN may be found in call records from other associated parties, or in a phone image. It is generally not found in a contemporary SIM image, since modern smart phones do not store a contact list on the SIM. In iPhone, the MSISDN can be found by association with iMessage and Facetime.

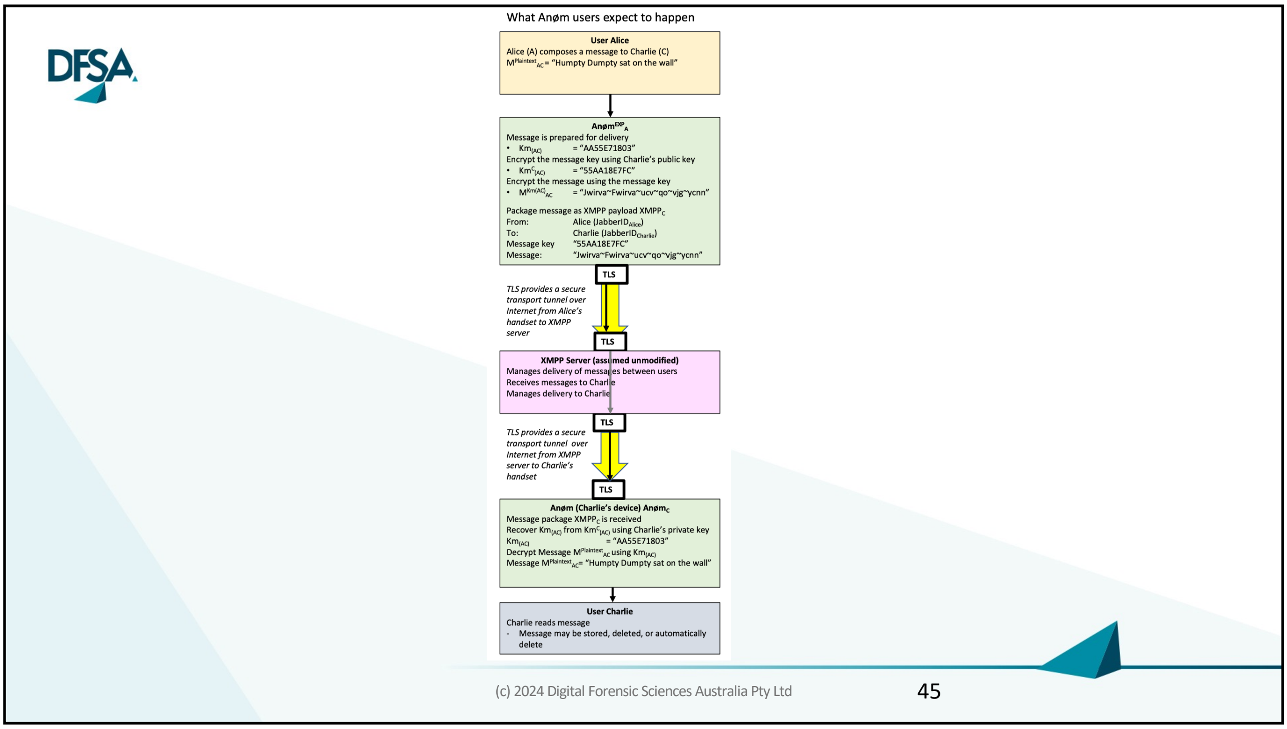
- **(Deprecated! Not recommended!)** For manual inspection the MSISDN may be found by calling a known phone which supports Caller ID.

Mobile Phone Forensics, 2021 © 2003-2021 M Sorell



ANØM

(c) 2024 Digital Forensic Sciences Australia Pty Ltd



What Anøm users expect to happen

User Alice
Alice (A) composes a message to Charlie (C)
$M^{Plaintext}_{AC}$ = “Humpty Dumpty sat on the wall”

Anøm$^{EXP}_{A}$
Message is prepared for delivery
- $Km_{(AC)}$ = “AA55E71803”

Encrypt the message key using Charlie’s public key
- $Km^{C}_{(AC)}$ = “55AA18E7FC”

Encrypt the message using the message key
- $M^{Km(AC)}_{AC}$ = “Jwirva~Fwirva~ucv~qo~vjg~ycnn”

Package message as XMPP payload $XMPP_C$
From: Alice ($JabberID_{Alice}$)
To: Charlie ($JabberID_{Charlie}$)
Message key “55AA18E7FC”
Message: “Jwirva~Fwirva~ucv~qo~vjg~ycnn”

TLS provides a secure transport tunnel over Internet from Alice’s handset to XMPP server

XMPP Server (assumed unmodified)
Manages delivery of messages between users
Receives messages to Charlie
Manages delivery to Charlie

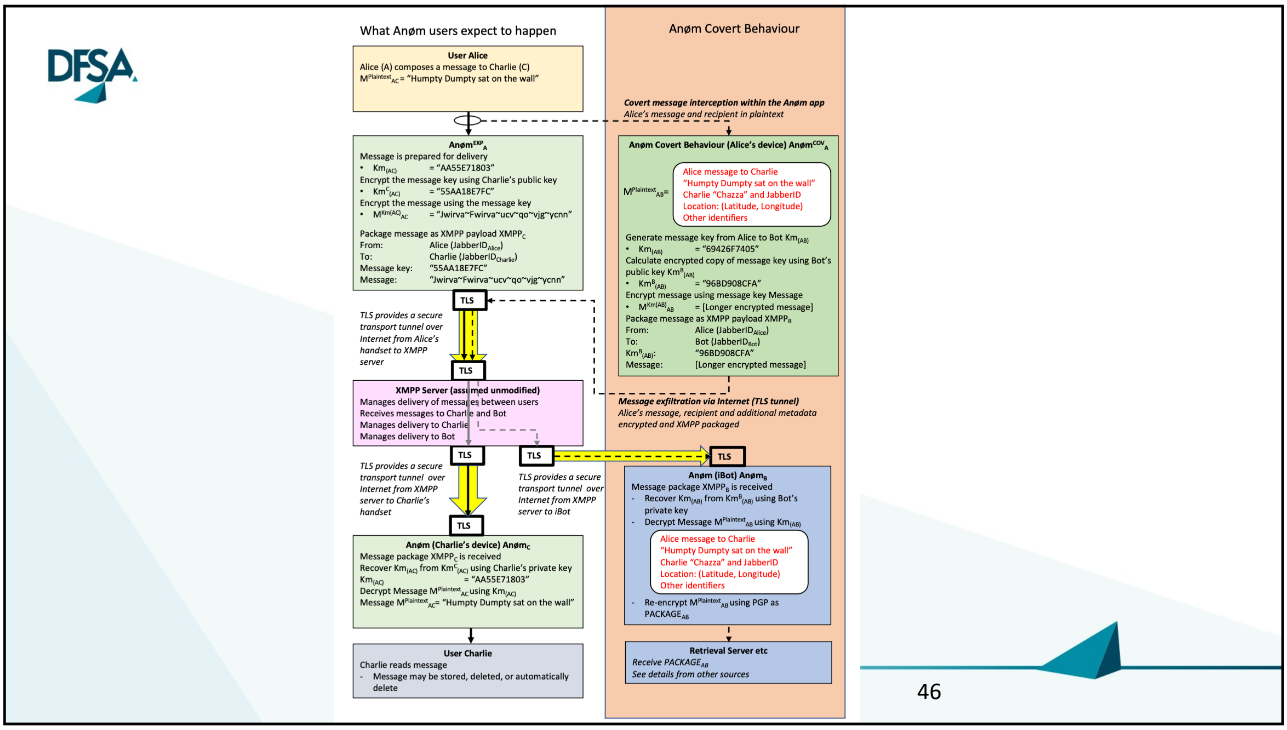
TLS provides a secure transport tunnel over Internet from XMPP server to Charlie’s handset

Anøm (Charlie’s device) Anøm$_C$
Message package $XMPP_C$ is received
Recover $Km_{(AC)}$ from $Km^{C}_{(AC)}$ using Charlie’s private key
$Km_{(AC)}$ = “AA55E71803”
Decrypt Message $M^{Plaintext}_{AC}$ using $Km_{(AC)}$
Message $M^{Plaintext}_{AC}$= “Humpty Dumpty sat on the wall”

User Charlie
Charlie reads message
- Message may be stored, deleted, or automatically delete

(c) 2024 Digital Forensic Sciences Australia Pty Ltd 45

45



What Anøm users expect to happen

User Alice
Alice (A) composes a message to Charlie (C)
$M^{Plaintext}_{AC}$ = “Humpty Dumpty sat on the wall”

Anøm$^{EXP}_{A}$
Message is prepared for delivery
- $Km_{(AC)}$ = “AA55E71803”

Encrypt the message key using Charlie’s public key
- $Km^{C}_{(AC)}$ = “55AA18E7FC”

Encrypt the message using the message key
- $M^{Km(AC)}_{AC}$ = “Jwirva~Fwirva~ucv~qo~vjg~ycnn”

Package message as XMPP payload $XMPP_C$
From: Alice ($JabberID_{Alice}$)
To: Charlie ($JabberID_{Charlie}$)
Message key: “55AA18E7FC”
Message: “Jwirva~Fwirva~ucv~qo~vjg~ycnn”

TLS provides a secure transport tunnel over Internet from Alice’s handset to XMPP server

XMPP Server (assumed unmodified)
Manages delivery of messages between users
Receives messages to Charlie and Bot
Manages delivery to Charlie
Manages delivery to Bot

TLS provides a secure transport tunnel over Internet from XMPP server to Charlie’s handset

TLS provides a secure transport tunnel over Internet from XMPP server to iBot

Anøm (Charlie’s device) Anøm$_C$
Message package $XMPP_C$ is received
Recover $Km_{(AC)}$ from $Km^{C}_{(AC)}$ using Charlie’s private key
$Km_{(AC)}$ = “AA55E71803”
Decrypt Message $M^{Plaintext}_{AC}$ using $Km_{(AC)}$
Message $M^{Plaintext}_{AC}$= “Humpty Dumpty sat on the wall”

User Charlie
Charlie reads message
- Message may be stored, deleted, or automatically delete

Anøm Covert Behaviour

Covert message interception within the Anøm app
Alice’s message and recipient in plaintext

Anøm Covert Behaviour (Alice’s device) Anøm$^{COV}_{A}$

$M^{Plaintext}_{AB}$=
Alice message to Charlie
“Humpty Dumpty sat on the wall”
Charlie “Chazza” and JabberID
Location: (Latitude, Longitude)
Other identifiers

Generate message key from Alice to Bot $Km_{(AB)}$
- $Km_{(AB)}$ = “69426F7405”

Calculate encrypted copy of message key using Bot’s public key $Km^{B}_{(AB)}$
- $Km^{B}_{(AB)}$ = “96BD908CFA”

Encrypt message using message key Message
- $M^{Km(AB)}_{AB}$ = [Longer encrypted message]

Package message as XMPP payload $XMPP_B$
From: Alice ($JabberID_{Alice}$)
To: Bot ($JabberID_{Bot}$)
$Km^{B}_{(AB)}$: “96BD908CFA”
Message: [Longer encrypted message]

Message exfiltration via Internet (TLS tunnel)
Alice’s message, recipient and additional metadata encrypted and XMPP packaged

Anøm (iBot) Anøm$_B$
Message package $XMPP_B$ is received
- Recover $Km_{(AB)}$ from $Km^{B}_{(AB)}$ using Bot’s private key
- Decrypt Message $M^{Plaintext}_{AB}$ using $Km_{(AB)}$

Alice message to Charlie
“Humpty Dumpty sat on the wall”
Charlie “Chazza” and JabberID
Location: (Latitude, Longitude)
Other identifiers

- Re-encrypt $M^{Plaintext}_{AB}$ using PGP as $PACKAGE_{AB}$

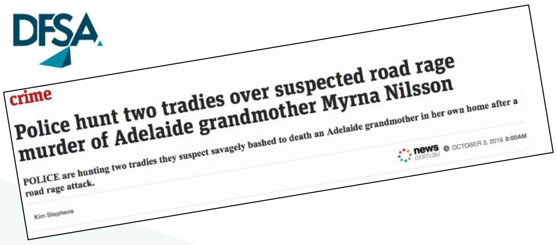
Retrieval Server etc
Receive $PACKAGE_{AB}$
See details from other sources

46

46

Apple Health Data
Lessons from 5 years of real data

- Luke Jennings – University of Adelaide
- Dr Hugo G Espinosa – Griffith University
- Dr Matthew Sorell – University of Adelaide



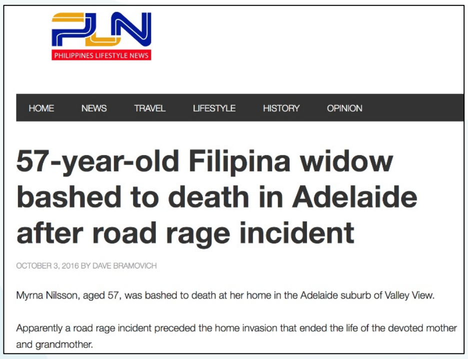
crime

Police hunt two tradies over suspected road rage murder of Adelaide grandmother Myrna Nilsson

news.com.au OCTOBER 3, 2016 8:00AM

POLICE are hunting two tradies they suspect savagely bashed to death an Adelaide grandmother in her own home after a road rage attack.

Kim Stephens

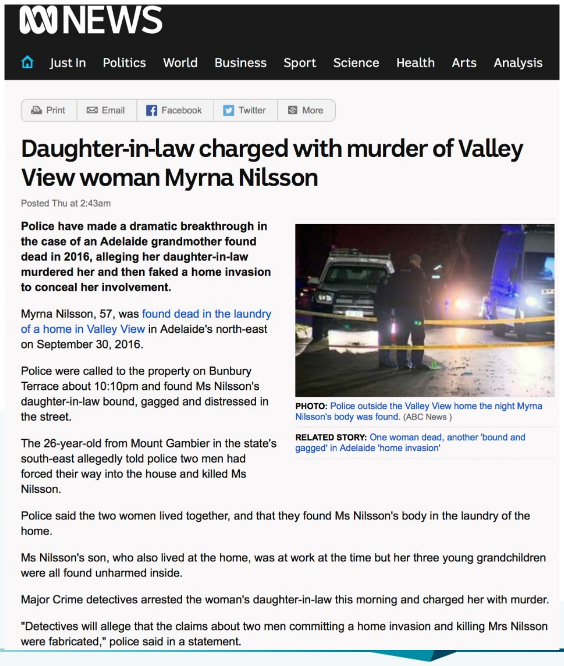


57-year-old Filipina widow bashed to death in Adelaide after road rage incident

OCTOBER 3, 2016 BY DAVE BRAMOVICH

Myrna Nilsson, aged 57, was bashed to death at her home in the Adelaide suburb of Valley View.

Apparently a road rage incident preceded the home invasion that ended the life of the devoted mother and grandmother.



Daughter-in-law charged with murder of Valley View woman Myrna Nilsson

Posted Thu at 2:43am

Police have made a dramatic breakthrough in the case of an Adelaide grandmother found dead in 2016, alleging her daughter-in-law murdered her and then faked a home invasion to conceal her involvement.

Myrna Nilsson, 57, was found dead in the laundry of a home in Valley View in Adelaide's north-east on September 30, 2016.

Police were called to the property on Bunbury Terrace about 10:10pm and found Ms Nilsson's daughter-in-law bound, gagged and distressed in the street.

The 26-year-old from Mount Gambier in the state's south-east allegedly told police two men had forced their way into the house and killed Ms Nilsson.

Police said the two women lived together, and that they found Ms Nilsson's body in the laundry of the home.

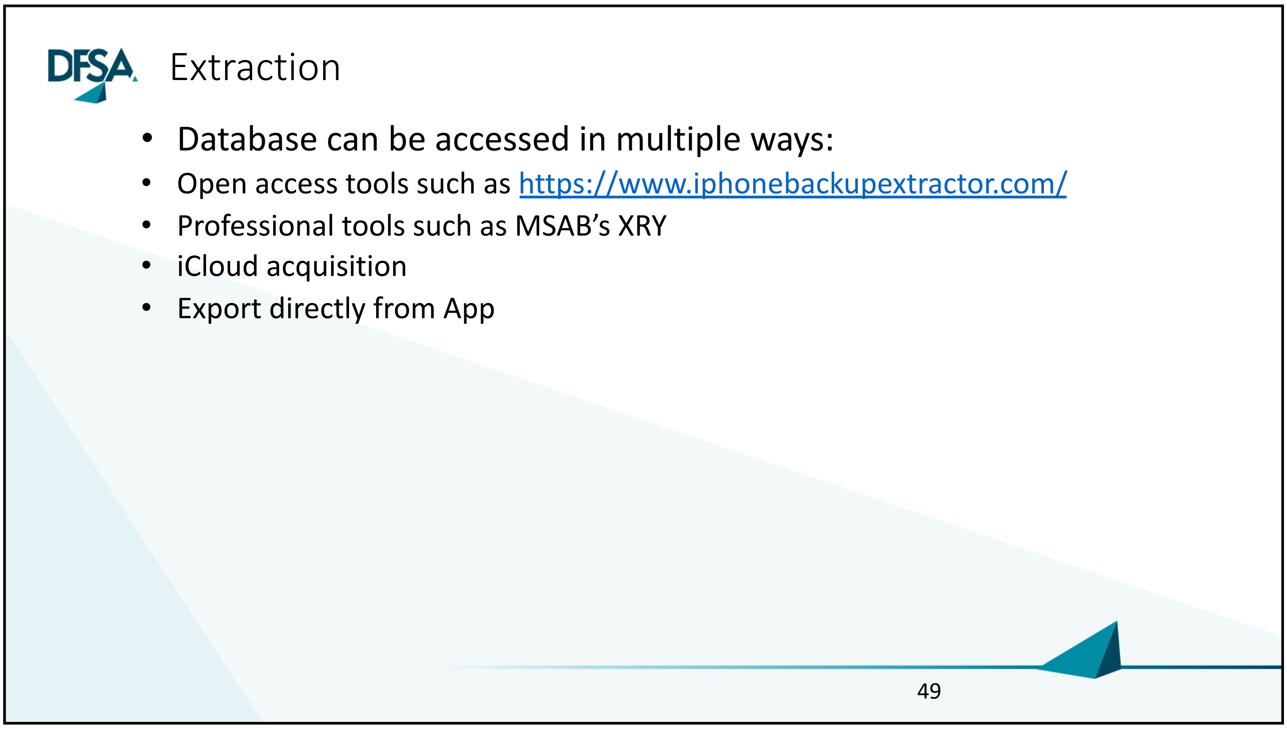
Ms Nilsson's son, who also lived at the home, was at work at the time but her three young grandchildren were all found unharmed inside.

Major Crime detectives arrested the woman's daughter-in-law this morning and charged her with murder.

"Detectives will allege that the claims about two men committing a home invasion and killing Mrs Nilsson were fabricated," police said in a statement.

PHOTO: Police outside the Valley View home the night Myrna Nilsson's body was found. (ABC News)

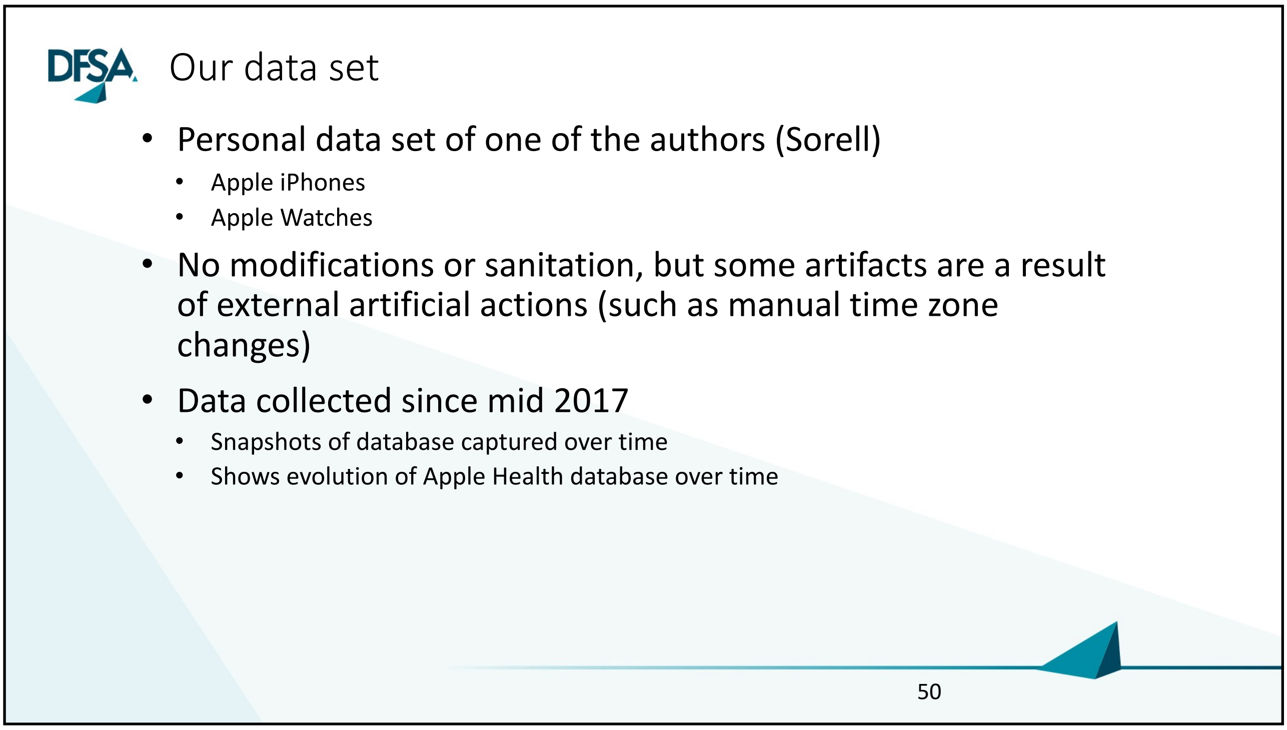
RELATED STORY: One woman dead, another 'bound and gagged' in Adelaide 'home invasion'



Extraction

- Database can be accessed in multiple ways:
- Open access tools such as https://www.iphonebackupextractor.com/
- Professional tools such as MSAB’s XRY
- iCloud acquisition
- Export directly from App

49



Our data set

- Personal data set of one of the authors (Sorell)
  - Apple iPhones
  - Apple Watches
- No modifications or sanitation, but some artifacts are a result of external artificial actions (such as manual time zone changes)
- Data collected since mid 2017
  - Snapshots of database captured over time
  - Shows evolution of Apple Health database over time

50

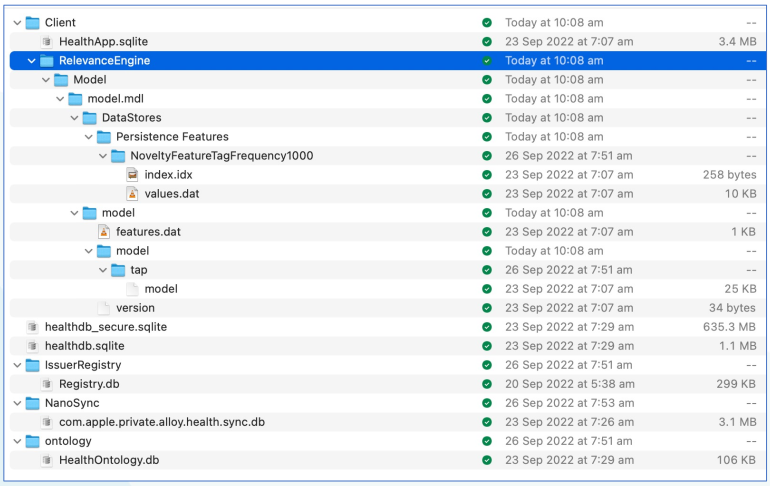
Use of my data set

- The data is real and invasive of privacy
- However, it is available to researchers, on request, when you undertake to uphold the following conditions:

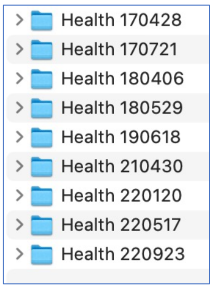
1. You do not publish my personal home address
2. You acknowledge the source data
3. You inform me of any work arising from the data, and supply a copy of publications
4. If you identify an underlying health condition, you let me know.

Contact: matthew@digitalforensicsciences.au

Inclusions

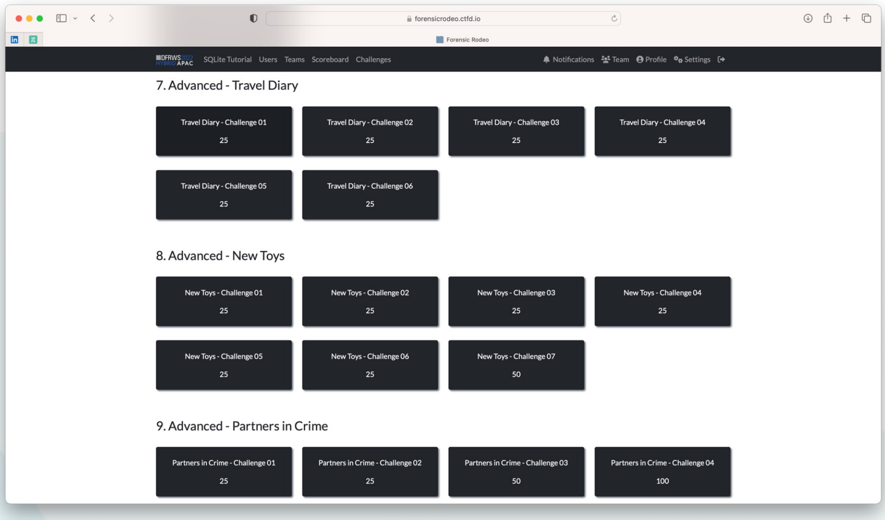


```
Client                                    Today at 10:08 am           --
    HealthApp.sqlite                      23 Sep 2022 at 7:07 am      3.4 MB
    RelevanceEngine                       Today at 10:08 am           --
        Model                             Today at 10:08 am           --
            model.mdl                     Today at 10:08 am           --
                DataStores                Today at 10:08 am           --
                    Persistence Features  Today at 10:08 am           --
                        NoveltyFeatureTagFrequency1000  26 Sep 2022 at 7:51 am  --
                            index.idx     23 Sep 2022 at 7:07 am      258 bytes
                            values.dat    23 Sep 2022 at 7:07 am      10 KB
                model                     Today at 10:08 am           --
                    features.dat          23 Sep 2022 at 7:07 am      1 KB
                    model                 Today at 10:08 am           --
                        tap               26 Sep 2022 at 7:51 am      --
                            model         23 Sep 2022 at 7:07 am      25 KB
                    version               23 Sep 2022 at 7:07 am      34 bytes
healthdb_secure.sqlite                    23 Sep 2022 at 7:29 am      635.3 MB
healthdb.sqlite                           23 Sep 2022 at 7:29 am      1.1 MB
IssuerRegistry                            26 Sep 2022 at 7:51 am      --
    Registry.db                           20 Sep 2022 at 5:38 am      299 KB
NanoSync                                  26 Sep 2022 at 7:53 am      --
    com.apple.private.alloy.health.sync.db  23 Sep 2022 at 7:26 am    3.1 MB
ontology                                  26 Sep 2022 at 7:51 am      --
    HealthOntology.db                     23 Sep 2022 at 7:29 am      106 KB
```



```
Health 170428
Health 170721
Health 180406
Health 180529
Health 190618
Health 210430
Health 220120
Health 220517
Health 220923
```

A CTF competition based on our data https://healthdata.ctfd.io



7. Advanced - Travel Diary

Travel Diary - Challenge 01 25

Travel Diary - Challenge 02 25

Travel Diary - Challenge 03 25

Travel Diary - Challenge 04 25

Travel Diary - Challenge 05 25

Travel Diary - Challenge 06 25

8. Advanced - New Toys

New Toys - Challenge 01 25

New Toys - Challenge 02 25

New Toys - Challenge 03 25

New Toys - Challenge 04 25

New Toys - Challenge 05 25

New Toys - Challenge 06 25

New Toys - Challenge 07 50

9. Advanced - Partners in Crime

Partners in Crime - Challenge 01 25

Partners in Crime - Challenge 02 25

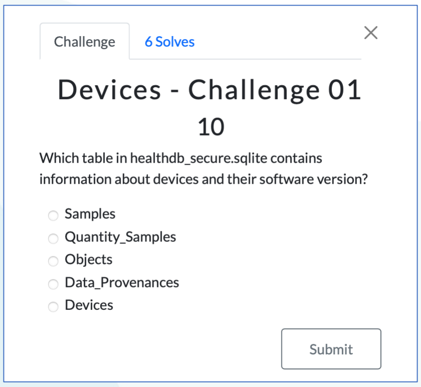
Partners in Crime - Challenge 03 50

Partners in Crime - Challenge 04 100

53

A CTF competition based on our data https://healthdata.ctfd.io

- The CTF is a guided tour of healthdb_secure.sqlite
- Scaffolded introduction to artefacts

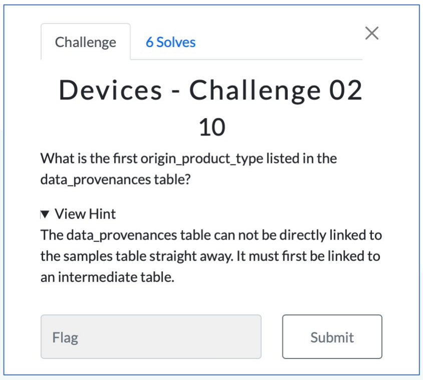


Devices - Challenge 01

10

Which table in healthdb_secure.sqlite contains information about devices and their software version?

○ Samples
○ Quantity_Samples
○ Objects
○ Data_Provenances
○ Devices



Devices - Challenge 02

10

What is the first origin_product_type listed in the data_provenances table?

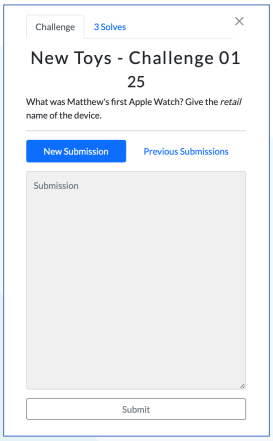
▼ View Hint

The data_provenances table can not be directly linked to the samples table straight away. It must first be linked to an intermediate table.

54

A CTF competition based on our data https://healthdata.ctfd.io

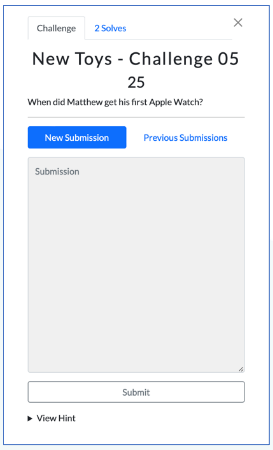
Guided “investigation” challenges



New Toys - Challenge 01

25

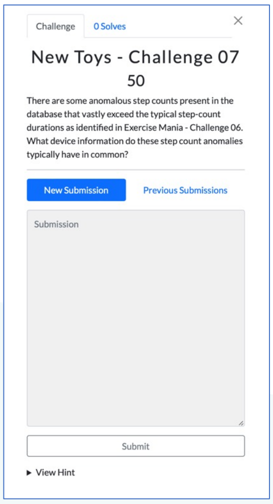
What was Matthew's first Apple Watch? Give the *retail* name of the device.



New Toys - Challenge 05

25

When did Matthew get his first Apple Watch?



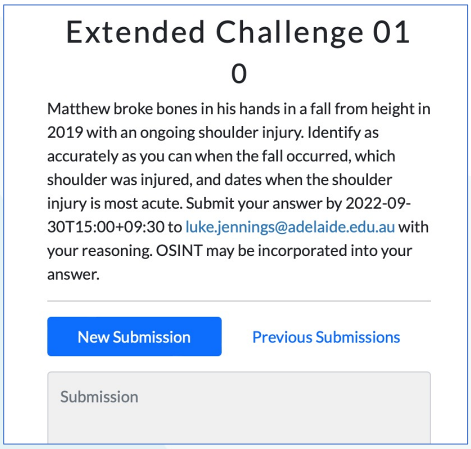
New Toys - Challenge 07

50

There are some anomalous step counts present in the database that vastly exceed the typical step-count durations as identified in Exercise Mania - Challenge 06. What device information do these step count anomalies typically have in common?

A CTF competition based on our data https://healthdata.ctfd.io

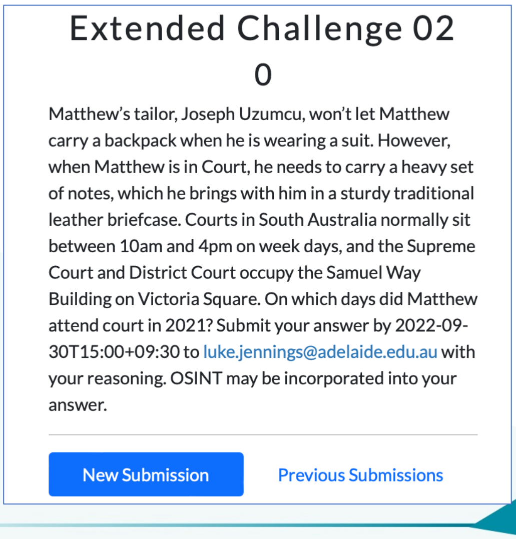
Open-ended challenges



Extended Challenge 01

0

Matthew broke bones in his hands in a fall from height in 2019 with an ongoing shoulder injury. Identify as accurately as you can when the fall occurred, which shoulder was injured, and dates when the shoulder injury is most acute. Submit your answer by 2022-09-30T15:00+09:30 to luke.jennings@adelaide.edu.au with your reasoning. OSINT may be incorporated into your answer.



Extended Challenge 02

0

Matthew’s tailor, Joseph Uzumcu, won’t let Matthew carry a backpack when he is wearing a suit. However, when Matthew is in Court, he needs to carry a heavy set of notes, which he brings with him in a sturdy traditional leather briefcase. Courts in South Australia normally sit between 10am and 4pm on week days, and the Supreme Court and District Court occupy the Samuel Way Building on Victoria Square. On which days did Matthew attend court in 2021? Submit your answer by 2022-09-30T15:00+09:30 to luke.jennings@adelaide.edu.au with your reasoning. OSINT may be incorporated into your answer.

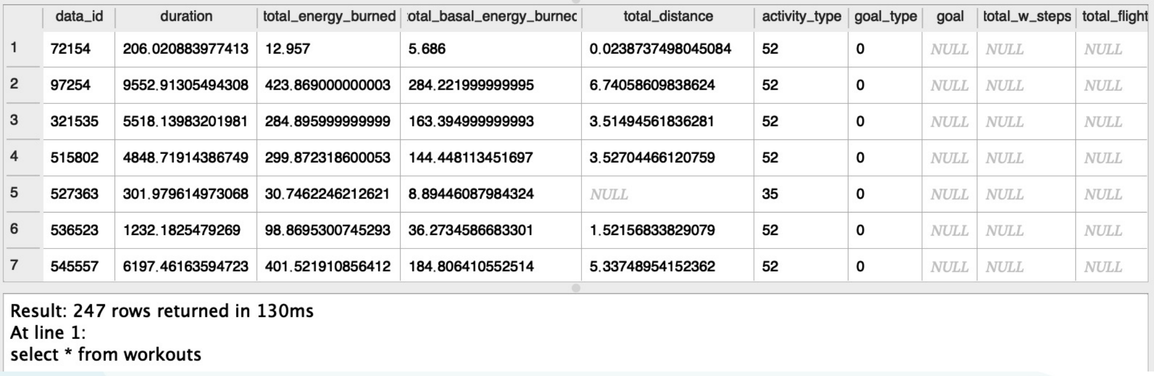
Exercise Mania

- By investigating a user’s workout data you can identify:
  - Preferred method of exercise, time, location and intensity
    - running,
    - cycling,
    - hiking,
    - rowing, etc.
- But all is not always as it seems…
    - Exercise triggers may not correctly identify exercise type
    - User may manually choose a similar exercise type

57

57

Exercise Mania



	data_id	duration	total_energy_burned	otal_basal_energy_burnec	total_distance	activity_type	goal_type	goal	total_w_steps	total_flight
1	72154	206.020883977413	12.957	5.686	0.0238737498045084	52	0	NULL	NULL	NULL
2	97254	9552.91305494308	423.869000000003	284.221999999995	6.74058609838624	52	0	NULL	NULL	NULL
3	321535	5518.13983201981	284.895999999999	163.394999999993	3.51494561836281	52	0	NULL	NULL	NULL
4	515802	4848.71914386749	299.872318600053	144.448113451697	3.52704466120759	52	0	NULL	NULL	NULL
5	527363	301.979614973068	30.7462246212621	8.89446087984324	NULL	35	0	NULL	NULL	NULL
6	536523	1232.1825479269	98.8695300745293	36.2734586683301	1.52156833829079	52	0	NULL	NULL	NULL
7	545557	6197.46163594723	401.521910856412	184.806410552514	5.33748954152362	52	0	NULL	NULL	NULL

```
Result: 247 rows returned in 130ms
At line 1:
select * from workouts
```

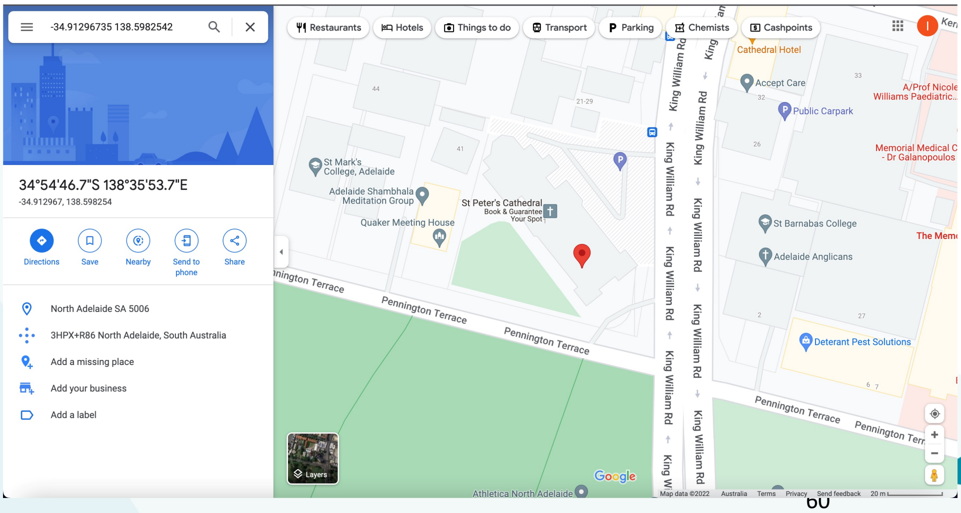
58

58

Exercise Mania

- Workout Types (activity_types)
  - Cycling = 13 (5 instances)
  - Hiking = 24 (1 instance)
  - Rowing = 35 (87 instances)
  - Running = 37 (1 instance)
  - Walking = 52 (153 instances)
- Preferred methods of exercise are Walking and Rowing.

Exercise Mania

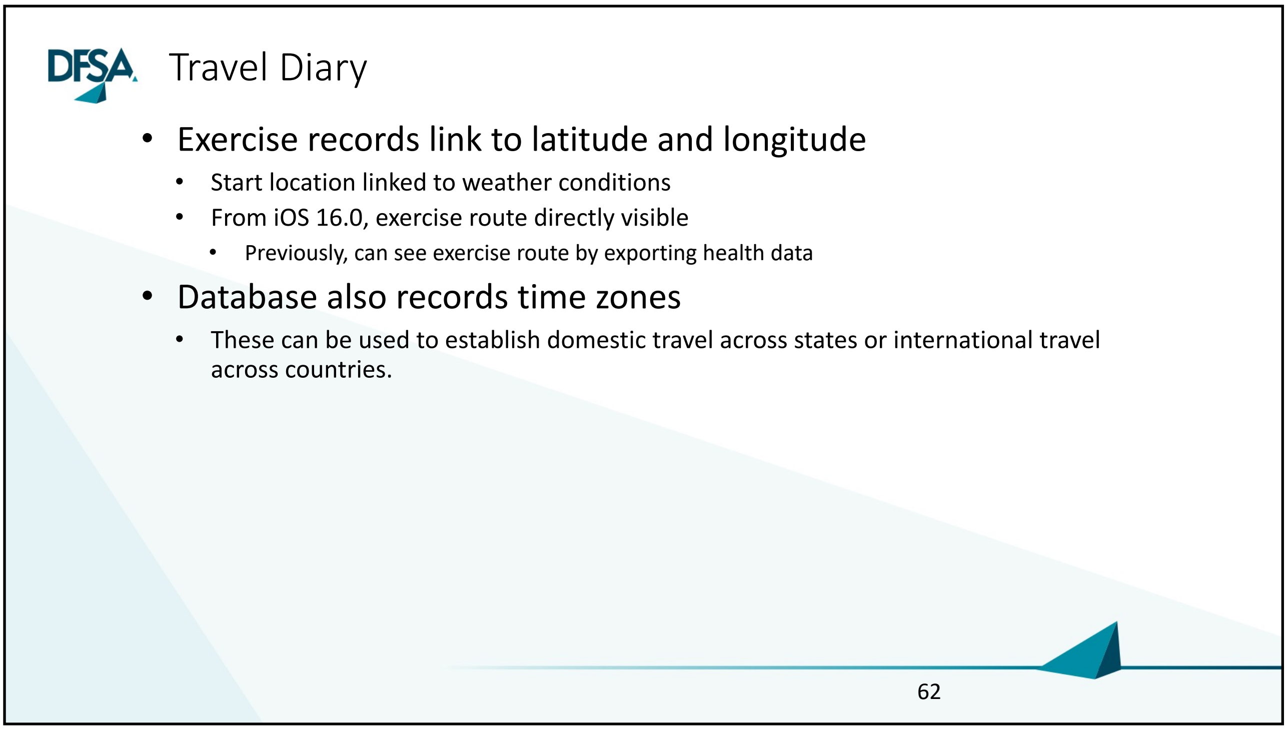


-34.91296735 138.5982542

34°54'46.7"S 138°35'53.7"E
-34.912967, 138.598254

North Adelaide SA 5006
3HPX+R86 North Adelaide, South Australia
Add a missing place
Add your business
Add a label

61

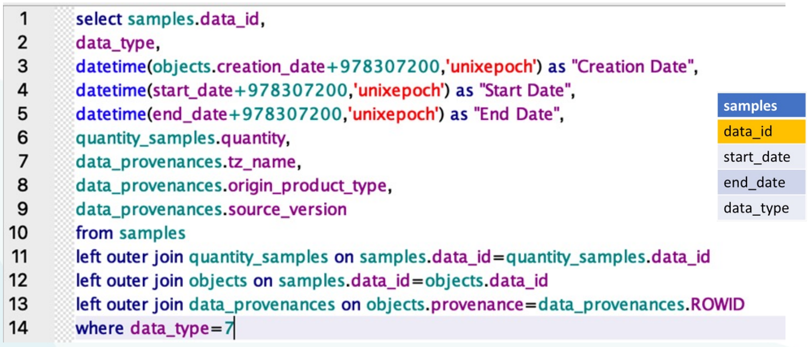


Travel Diary

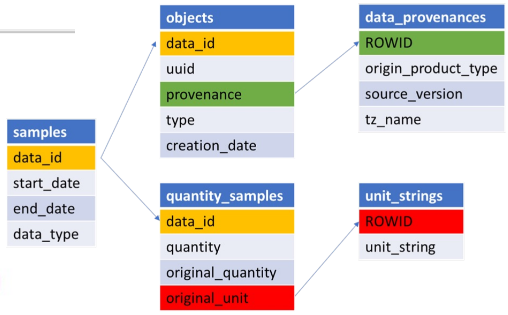
- Exercise records link to latitude and longitude
  - Start location linked to weather conditions
  - From iOS 16.0, exercise route directly visible
    - Previously, can see exercise route by exporting health data
- Database also records time zones
  - These can be used to establish domestic travel across states or international travel across countries.

62

Timezone extraction

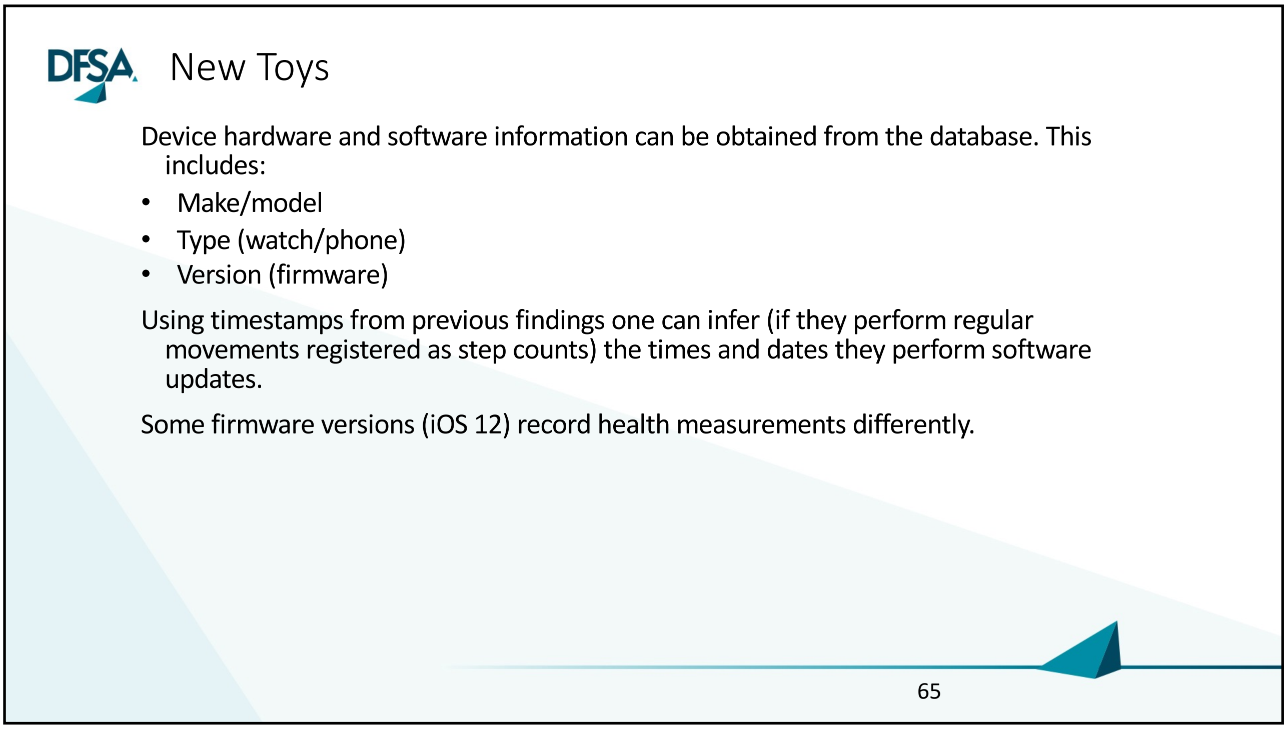


```
select samples.data_id,
data_type,
datetime(objects.creation_date+978307200,'unixepoch') as "Creation Date",
datetime(start_date+978307200,'unixepoch') as "Start Date",
datetime(end_date+978307200,'unixepoch') as "End Date",
quantity_samples.quantity,
data_provenances.tz_name,
data_provenances.origin_product_type,
data_provenances.source_version
from samples
left outer join quantity_samples on samples.data_id=quantity_samples.data_id
left outer join objects on samples.data_id=objects.data_id
left outer join data_provenances on objects.provenance=data_provenances.ROWID
where data_type=7
```



Travel Diary

Time zone	Timestamp UTC	Timestamp (local)	Status	Ground truth
Australia/Adelaide	25/6/2017 20:59	26/6/2017 6:29	Departure	Adelaide 06:25 (local)to Hong Kong 13:45 (local)
Asia/Hong_Kong	26/6/2017 6:30	26/6/2017 14:30	Arrival	
Asia/Hong_Kong	27/6/2017 2:08	27/6/2017 10:08	Departure	Hong Kong 00:25 (local) to Helsinki 06:00 (local)
Europe/Helsinki	27/6/2017 2:39	27/6/2017 5:39	Arrival	
Europe/Helsinki	29/6/2017 12:05	29/6/2017 15:05	Departure	Ferry to Tallinn 14:00-16:00 (local)
Europe/Tallinn	29/6/2017 12:22	29/6/2017 15:22	Arrival	
Europe/Tallinn	16/7/2017 14:12	16/7/2017 17:12	Departure	Ferry to Helsinki 16:00-18:00 (local)
Europe/Helsinki	16/7/2017 14:22	16/7/2017 17:22	Arrival	
Europe/Helsinki	17/7/2017 21:08	18/7/2017 0:08	Departure	Dep 16/7 20:55 UTC Helsinki Arr 17/7 08:40 UTC Singapore Dep 17/7 11:55 UTC Singapore Arr 17/7 19:20 UTC Melbourne Dep 17/7 21:30 UTC Melbourne Arr 17/7 22:50 UTC Adelaide
Australia/Adelaide	17/7/2017 22:52	18/7/2017 8:22	Arrival	



New Toys

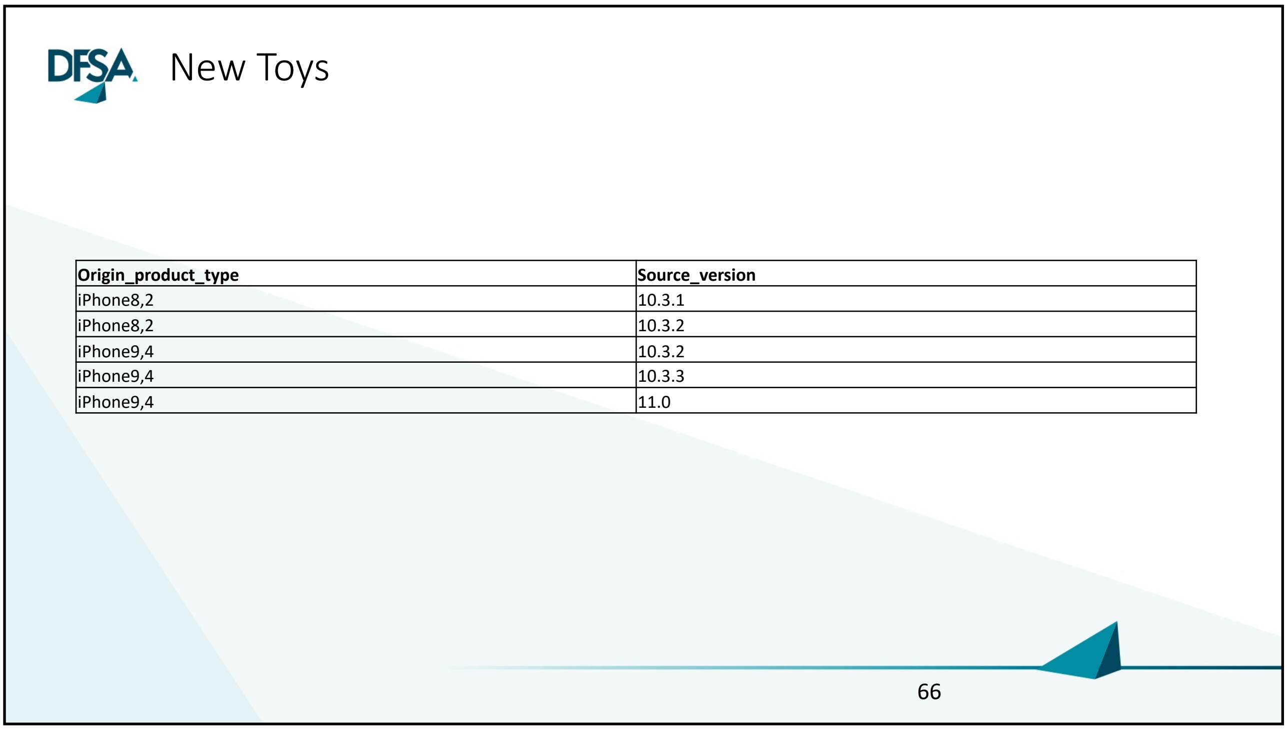
Device hardware and software information can be obtained from the database. This includes:

- Make/model
- Type (watch/phone)
- Version (firmware)

Using timestamps from previous findings one can infer (if they perform regular movements registered as step counts) the times and dates they perform software updates.

Some firmware versions (iOS 12) record health measurements differently.

65



New Toys

Origin_product_type	Source_version
iPhone8,2	10.3.1
iPhone8,2	10.3.2
iPhone9,4	10.3.2
iPhone9,4	10.3.3
iPhone9,4	11.0

66

The Quintilian Project

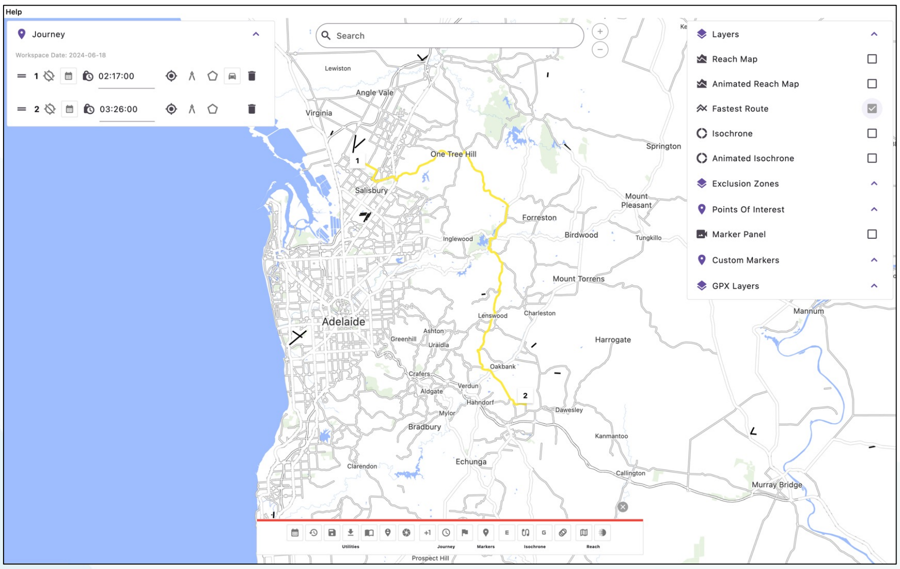
Visualising Reachable Areas
Developments and Challenges

Dr Matthew Sorell, Principal Consultant and CTO

Bailey Heading, Algorithm Developer

matthew@digitalforensicsciences.au

Getting from A to B



Help

Journey

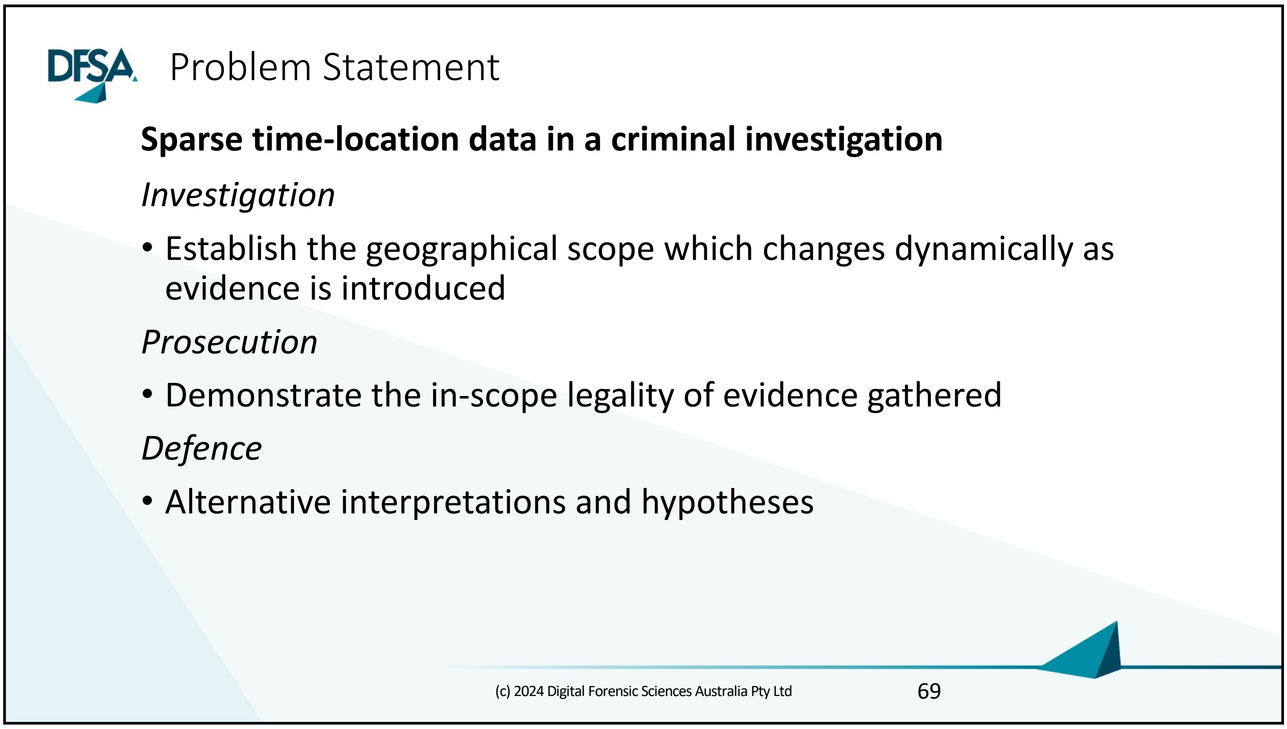
Workspace Date: 2024-06-18

1 02:17:00

2 03:26:00

Layers

- Reach Map □
- Animated Reach Map □
- Fastest Route ☑
- Isochrone □
- Animated Isochrone □
- Exclusion Zones
- Points Of Interest
- Marker Panel □
- Custom Markers
- GPX Layers



Problem Statement

Sparse time-location data in a criminal investigation

Investigation

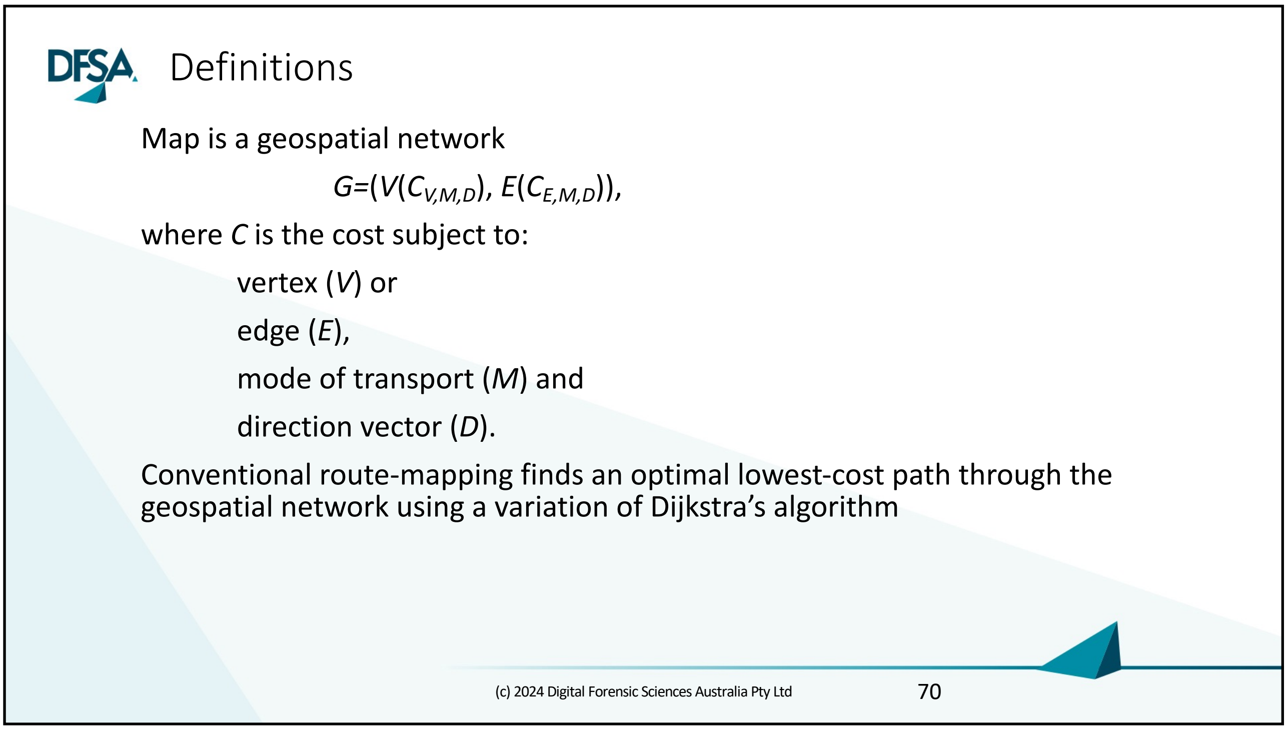
- Establish the geographical scope which changes dynamically as evidence is introduced

Prosecution

- Demonstrate the in-scope legality of evidence gathered

Defence

- Alternative interpretations and hypotheses



Definitions

Map is a geospatial network

$$G=(V(C_{V,M,D}), E(C_{E,M,D})),$$

where *C* is the cost subject to:

vertex (*V*) or

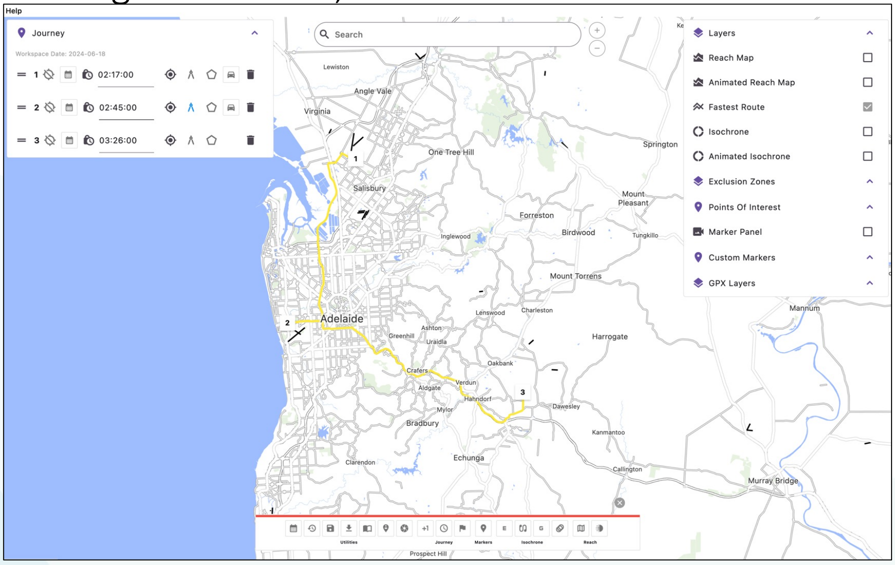
edge (*E*),

mode of transport (*M*) and

direction vector (*D*).

Conventional route-mapping finds an optimal lowest-cost path through the geospatial network using a variation of Dijkstra’s algorithm

Getting from A to B, via C



Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:45:00

3 03:26:00

Layers

- Reach Map ☐
- Animated Reach Map ☐
- Fastest Route ☑
- Isochrone ☐
- Animated Isochrone ☐
- Exclusion Zones
- Points Of Interest
- Marker Panel ☐
- Custom Markers
- GPX Layers

Reach

- Test whether V_1 is reachable from V_0 in the available time $\Delta t = (t_1 - t_0)$.
- Define the **surplus** S as Δt - $t_{\min(0\text{-}1)}$ which is ≥ 0 if the path is feasible.
- Force the path from V_0 to V_1 to visit intermediate node $V_{01.}$

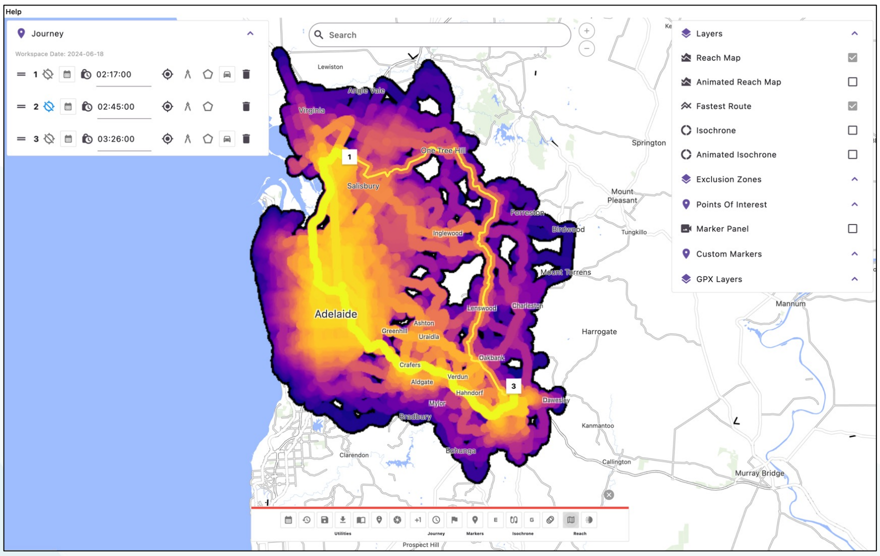
$$t_{\min(0\text{-}1)} = t_{\min(0\text{-}01)} + t_{\min(01\text{-}1)}$$

- Path is feasible if its surplus is non-negative

$$S_{0\text{-}01\text{-}1} = \Delta t - (t_{\min(0\text{-}01)} + t_{\min(01\text{-}1)}) \geq 0$$

The set of all vertices R_{01} which satisfy the feasibility criterion is the **reach** between V_0 and V_1 within the cost constraint of the time available.

Reach



Help

Journal

Workspace Date: 2024-06-18

1 02:17:00

2 02:45:00

3 03:26:00

Layers

Reach Map ☑

Animated Reach Map □

Fastest Route ☑

Isochrone □

Animated Isochrone □

Exclusion Zones

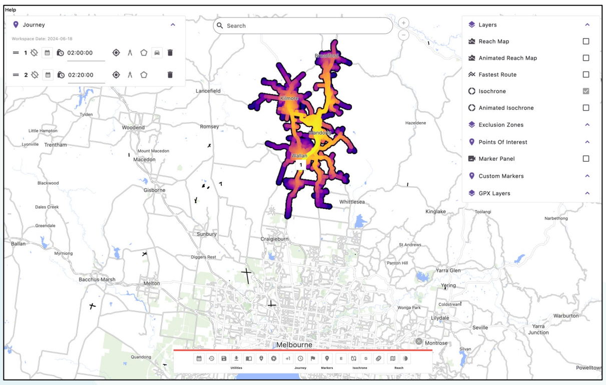
Points Of Interest

Marker Panel □

Custom Markers

GPX Layers

Isochrones as a special case



Journal

Workspace Date: 2024-06-18

1 02:00:00

2 02:20:00

Layers

Reach Map □

Animated Reach Map □

Fastest Route □

Isochrone ☑

Animated Isochrone □

Exclusion Zones

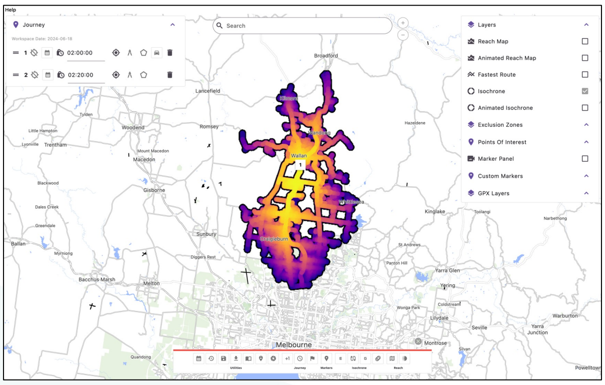
Points Of Interest

Marker Panel □

Custom Markers

GPX Layers

Outgoing exo-isochrone



Journal

Workspace Date: 2024-06-18

1 02:00:00

2 02:20:00

Layers

Reach Map □

Animated Reach Map □

Fastest Route □

Isochrone ☑

Animated Isochrone □

Exclusion Zones

Points Of Interest

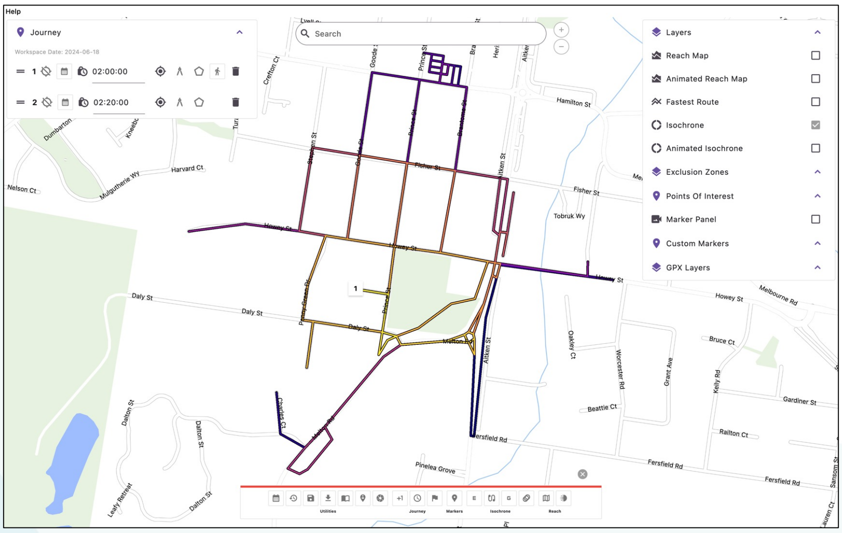
Marker Panel □

Custom Markers

GPX Layers

Incoming endo-isochrone

Round-trip *hobbito**-isochrone



Help

Journey

Workspace Date: 2024-06-18

1 02:00:00

2 02:20:00

Layers

Reach Map ☐

Animated Reach Map ☐

Fastest Route ☐

Isochrone ☑

Animated Isochrone ☐

Exclusion Zones

Points Of Interest

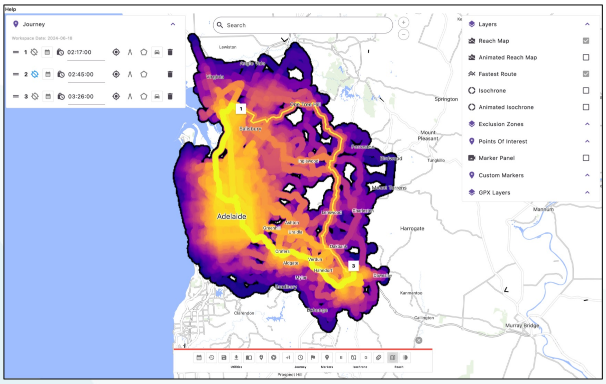
Marker Panel ☐

Custom Markers

GPX Layers

*Tolkein, JRR, The Hobbit, or "There and Back Again"

Waypoints



Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:45:00

3 03:26:00

Layers

Reach Map ☑

Animated Reach Map ☐

Fastest Route ☑

Isochrone ☐

Animated Isochrone ☐

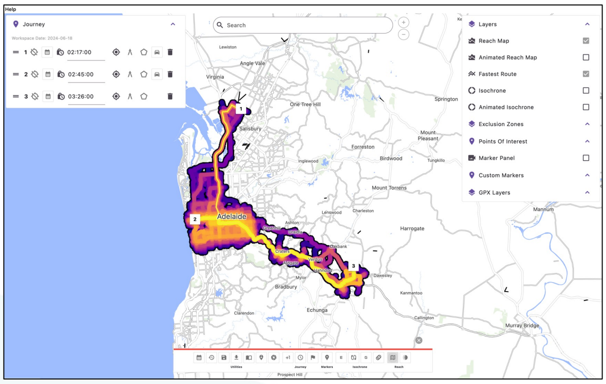
Exclusion Zones

Points Of Interest

Marker Panel ☐

Custom Markers

GPX Layers



Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:45:00

3 03:26:00

Layers

Reach Map ☑

Animated Reach Map ☐

Fastest Route ☑

Isochrone ☐

Animated Isochrone ☐

Exclusion Zones

Points Of Interest

Marker Panel ☐

Custom Markers

GPX Layers

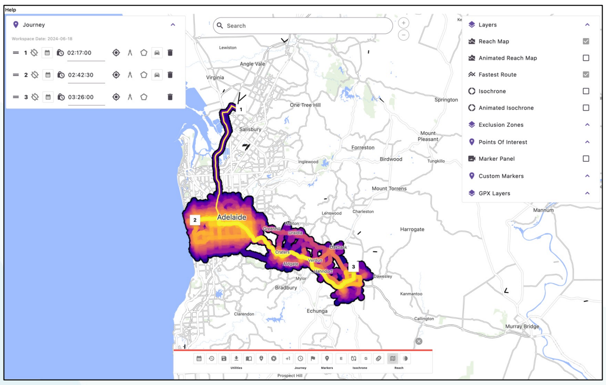
$$R = R_{0\text{-}1} \cup R_{1\text{-}2}$$

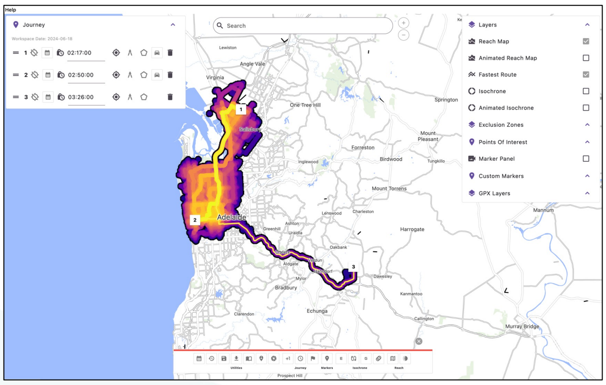
Using Bellman's Principle of Optimality: $S = \max\,(S_{0\text{-}1}, S_{1\text{-}2})$

Arrival and Departure Times

- For each waypoint, need to consider
  - Earliest and Latest Arrival
  - Earliest and Latest Departure
- Considerations
  - Fastest path in and out of waypoint
  - Known event at waypoint (eg phone call start and end time)
  - Dwell time
- The model allows earliest departure *before* latest arrival

Waypoint with unknown time





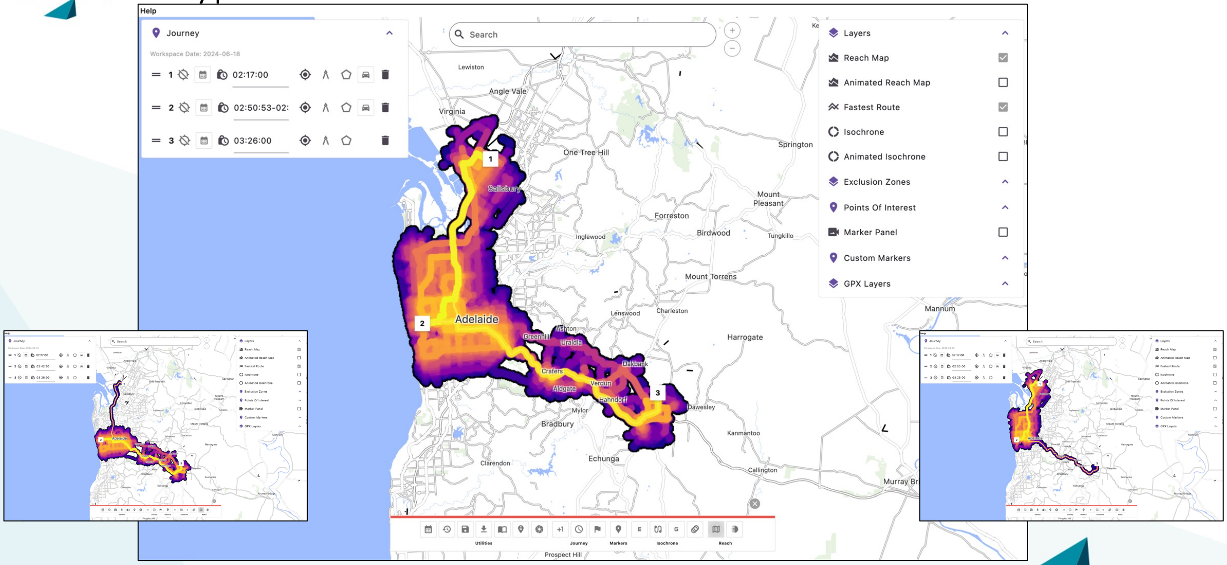
Earliest arrival at waypoint:
Fastest path from source to waypoint
Maximum reach from waypoint to destination

Earliest Arrival
Earliest Departure

Latest Arrival
Latest Departure

Latest arrival at waypoint:
Maximum reach from source to waypoint
Fastest path from waypoint to destination

Waypoint with unknown time



Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:50:53-02:

3 03:26:00

Layers

Reach Map ☑

Animated Reach Map ☐

Fastest Route ☑

Isochrone ☐

Animated Isochrone ☐

Exclusion Zones

Points Of Interest

Marker Panel ☐

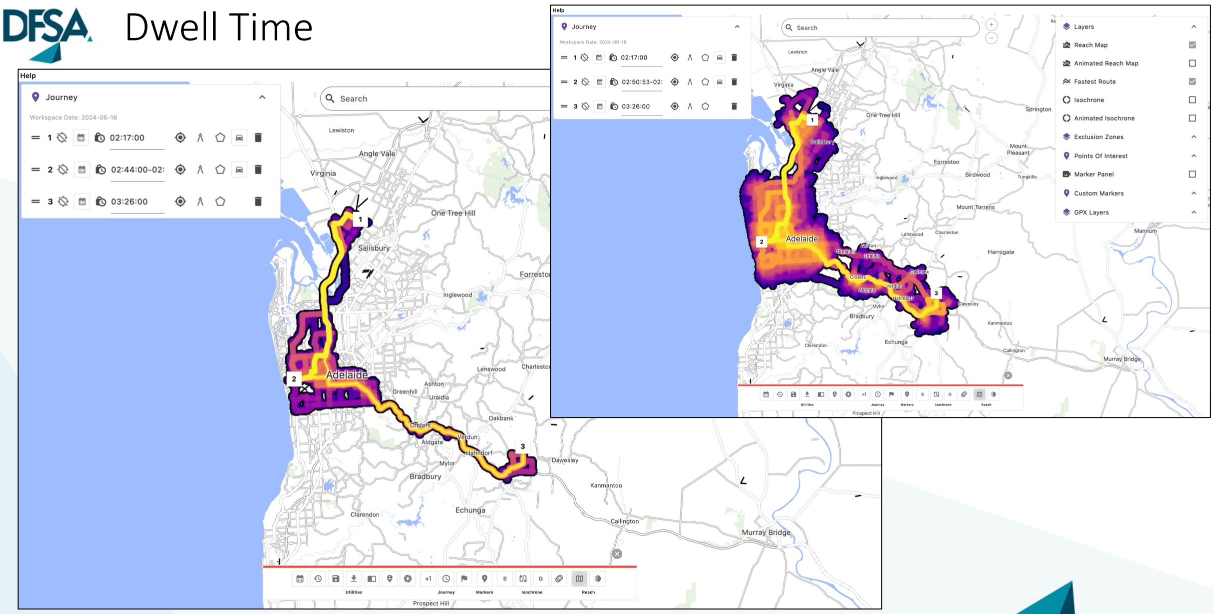
Custom Markers

GPX Layers

79

79

Dwell Time



Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:44:00-02:

3 03:26:00

Help

Journey

Workspace Date: 2024-06-18

1 02:17:00

2 02:50:53-02:

3 03:26:00

Layers

Reach Map ☑

Animated Reach Map ☐

Fastest Route ☑

Isochrone ☐

Animated Isochrone ☐

Exclusion Zones

Points Of Interest

Marker Panel ☐

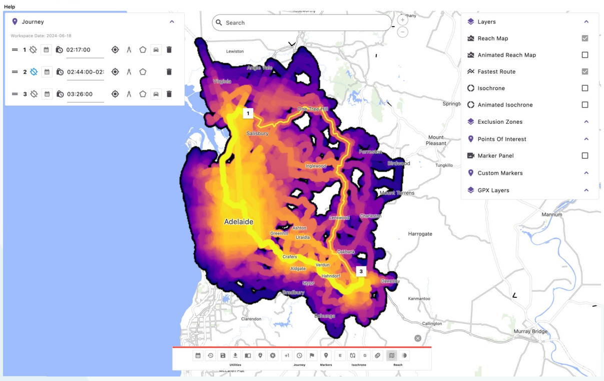
Custom Markers

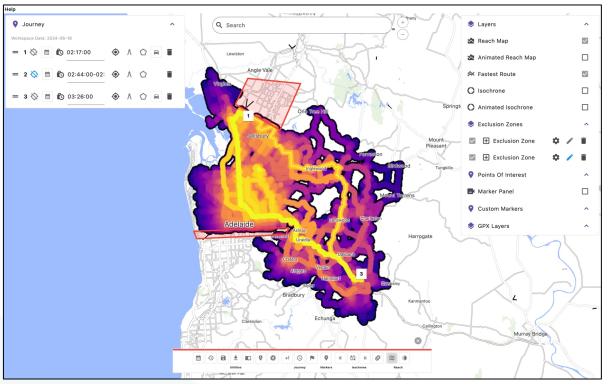
GPX Layers

80

80

Excluded zones





Exclusion is a modified edge cost in

- Known road closure / confirmed non sighting
- Vehicle height restriction

Other reasons for modified costs

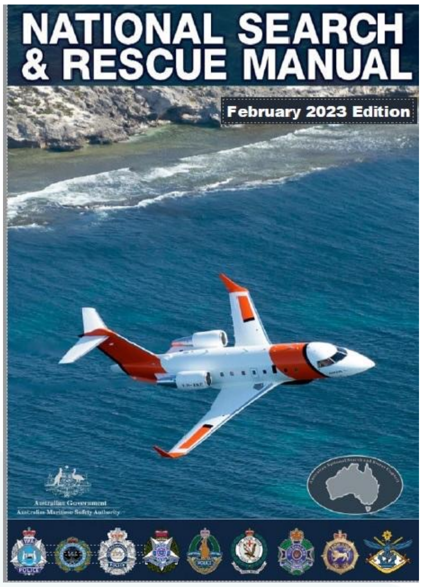
- Transportation mode
- Time of day / live traffic conditions

GIS challenges

- Prototype relies on 2018 OSM maps
- Primary and secondary roads are mostly up to date
- Tertiary tracks are largely missing
- Undocumented tracks are … undocumented
  - This includes a pedestrian jumping fences
- Roads may be closed
- A pedestrian track might be traversable by vehicle
- Speed limits and one-way road rules may not apply

Applications

- Missing persons
- Search and rescue
- Applicability of traces to investigation
- Targeted review of CCTV
- Customs
- Strategic surveillance bottleneck analysis
- Re-routing around disruptions



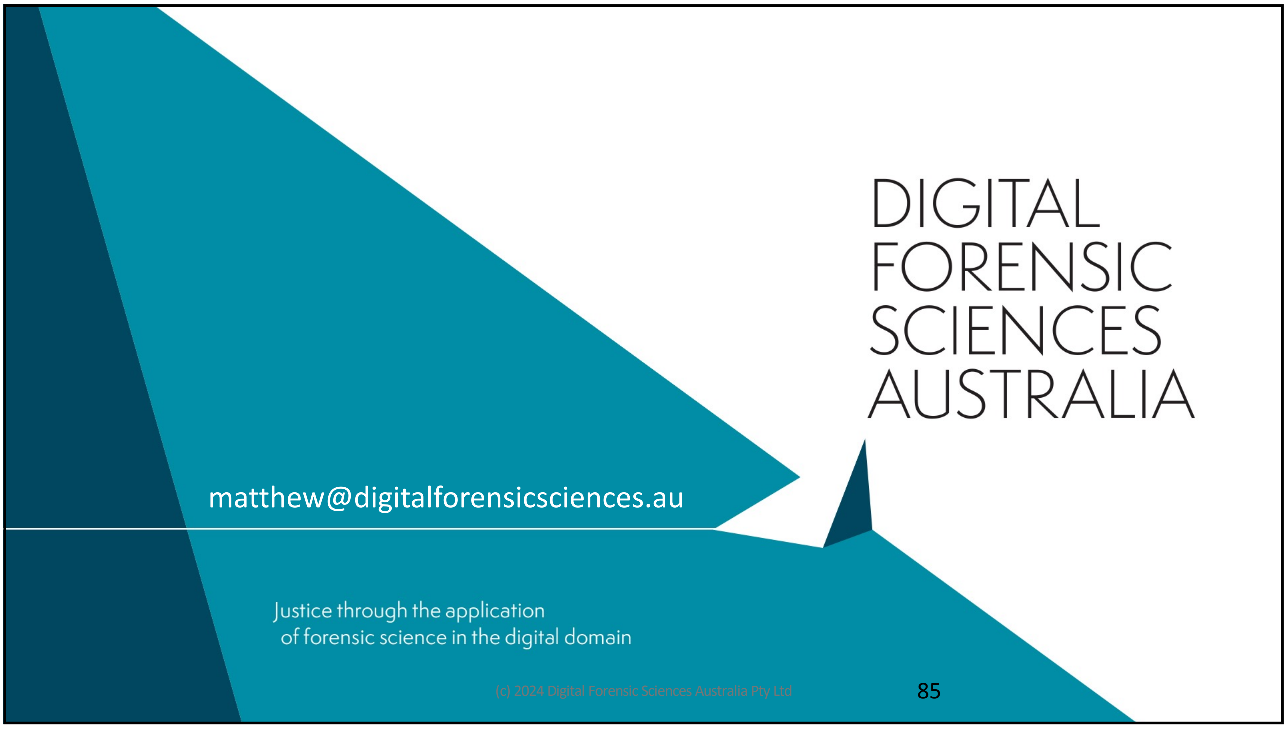
NATIONAL SEARCH & RESCUE MANUAL

February 2023 Edition

Delivery

Reach map needs to support the application

- Manual interaction by experts
- Automated data ingestion and operational command and control
- Rules-based templates for specific search contexts
- Potential use of machine learning to support investigation?



DIGITAL
FORENSIC
SCIENCES
AUSTRALIA

matthew@digitalforensicsciences.au

Justice through the application
of forensic science in the digital domain

85

85