UNSW SYDNEY | Australia's Global University

sec edu

security engineering capability

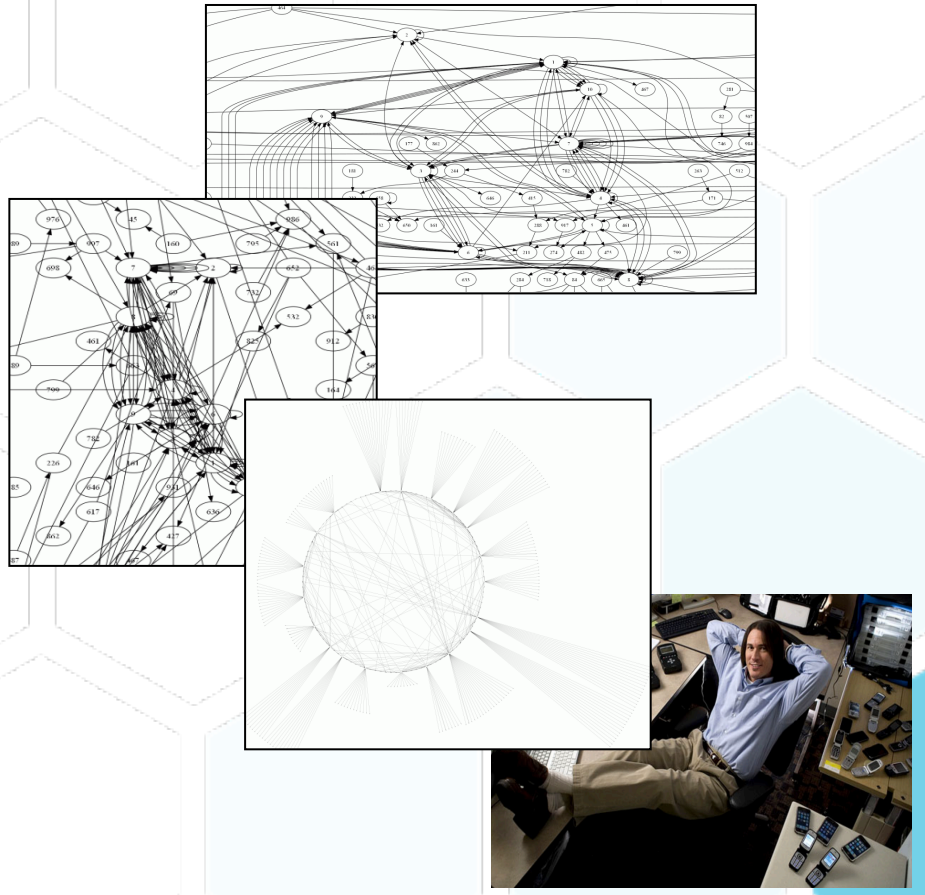
COMP6445 – Digital Forensics

Term 3 2019 - Week 6 part 2

21 October 2019

Agenda

- Introduction
- Key challenges (selected)
  - Time
  - Volume of extraneous data
  - Translating IP address to a person or geographical address
- PCAP and Netflow



Digital Forensic Science in Networked Environments (Network Forensics)

Definition:

The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities[1]

1. A roadmap for Digital Forensic Research DFRWS 2001
See http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

DFRWS – Network forensic challenges

- Time H
- Performance

- Complexity
  - Tools across multiple environments
  - Correlation

- Collection
  - Who, when and what

- Paradigms
  - Intelligence, network operations, law enforcement

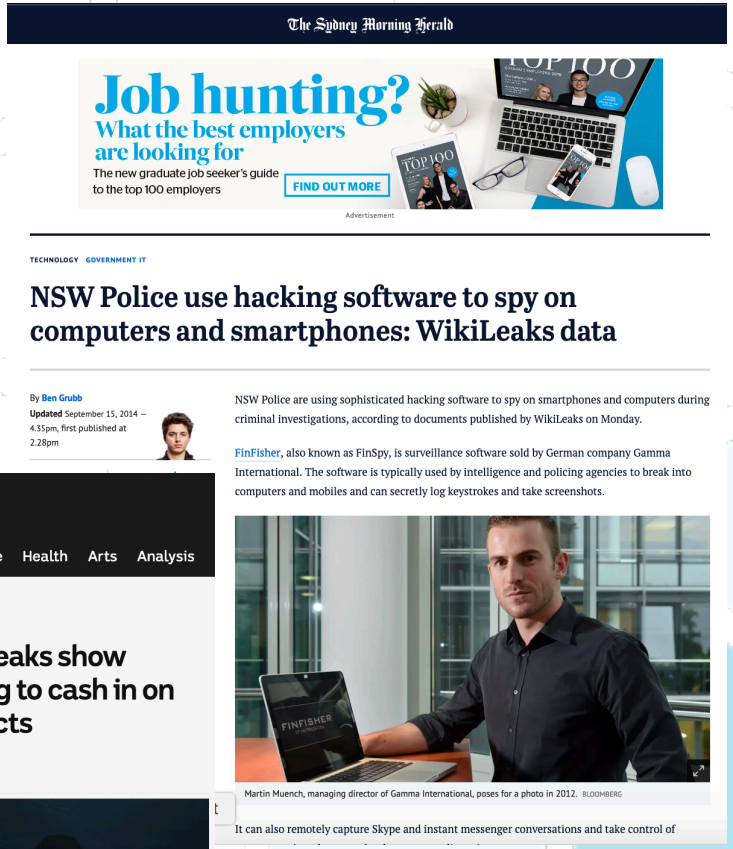
- Collaboration
- Legal hurdle
- Emerging technologies

Speed and Volume H

Translating IP address to person or geographical address H

Interception and assistance

- For this course, at the Unclassified level, I will steer clear of interception and assistance
- Much has been made available by whistleblowers e.g. Wikileaks



1. See https://www.smh.com.au/technology/nsw-police-use-hacking-software-to-spy-on-computers-and-smartphones-wikileaks-data-20140915-10h530.html
2. See https://www.abc.net.au/news/2015-07-28/wikileaks-reveals-australian-companies-selling-spyware/6652184

Common interactions to be analysed

- IP packets
- email
- Telephone & SMS
- non-IP protcols e.g. Zigbee, Modbus, H.323, H.450, etc
- “Old” protocols e.g. SNA, X.25, etc
- Sneaker and other “dark”nets

This is almost always done by incident response and forensic activity is “merely” analysing the result

This represents the most significant portion of my case load forensic activity

This represents an increasing proportion of my advisory load activity

A word of warning

- When using cloud-based tools, understand their terms of service and how they affect your responsibilities as an expert:
  - Must keep any materials provided to you confidential;
  - The Court's copyright exemption does not apply to your own pre-trial investigations.

Your Content in our Services

Access to the public PacketTotal website is free of charge, with the exception of any specific pricing conditions that may apply to certain Services

You retain all ownership rights in any submission you may make and you confirm that you are the original owner of any content you submit or that you have the necessary rights and permissions to authorise us to use your content. In particular, you promise that you have obtained the permission of all of the people featured or referred to in the Content (and if they are under 18 their parents or guardians as well) to our use of the Content on the Services. You agree to give us evidence of all such rights and permissions if so requested by us.

When you upload or otherwise submit content, you give PacketTotal (and those we work with) a worldwide, royalty free, irrevocable and transferable licence to use, edit, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content.

If you do not want the content provided by you to PacketTotal to be disclosed in the manner set out in these Terms or in the Privacy Policy, do not send it/share it with PacketTotal.

https://packettotal.com/tos.html

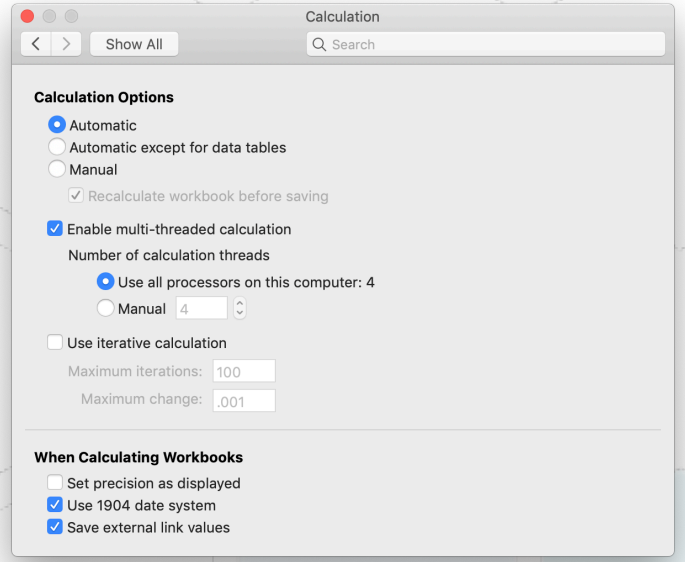
Time

A real scenario (details changed):

1. Suspect claims an SMS interaction gave consent for sex and videoing the act
2. CCR time taken from source using UTC i.e. GMT
3. LELO in Sydney saves at work using Windows;
4. LELO takes home and opens on Mac. Saves as text and sends to Police e.g. 10/3/14 (10Mar14)
   - Error of 1462 days i.e. 4 years
5. Corrects for UTC by adding +10 hours to all times but leaves a GMT designator
   - Okay for winter
6. Police attempt to match with Gmail and Hotmail emails in PST (GMT-8). Instead of adding 8hrs to get to GMT time, they subtract 8hrs
7. Police can't match the emails with SMS and conclude that the exculpatory messages were not sent/received

⇩

It turns out that the LELO has been "working from home" for several years



Activity: what is the error i.e. the difference between Sydney time?

Volume of extraneous data

- Convergence of big data and cyber

- The two questions:
  1. How do you identify the important data?; and
  2. How do you persuade others that you have adequately consider the other data?

- Visualisation can help
  - Core is data in either:
    - From → To → Time
    - From → To → Number
  - Log2timeline[1] produced tagged data. Useful for email, browsing history, etc
  - Graphviz[2] is an open source tool that us useful for visualising data, especially data that is From → To → No. such as IP, email, tel, SMS, etc. Useful for firewall and web server logs and netflows
  - Commercial software such as Analyst Notebook, Cognos, Tableau, Palitir, etc also are useful

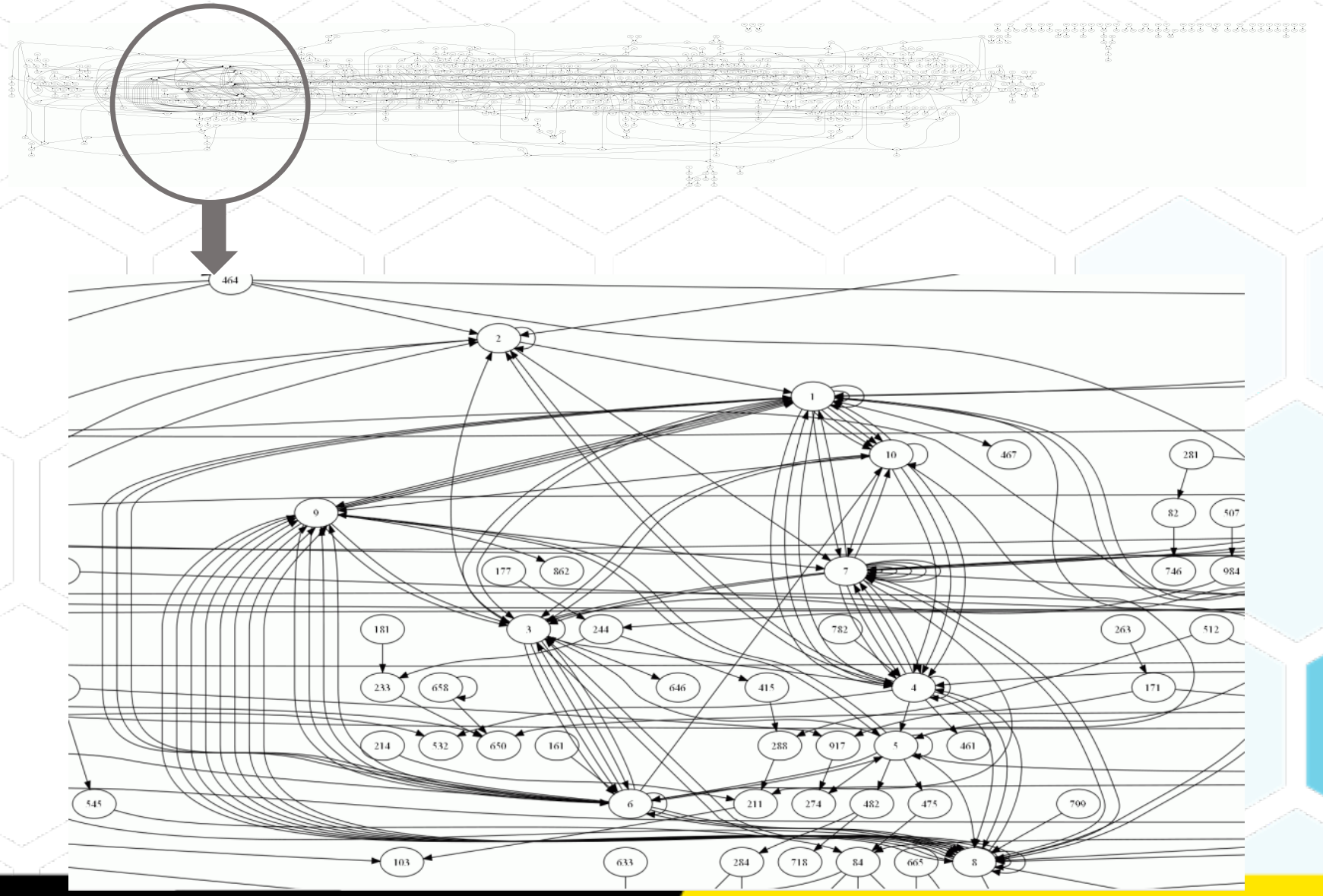
ACTIVITY for home

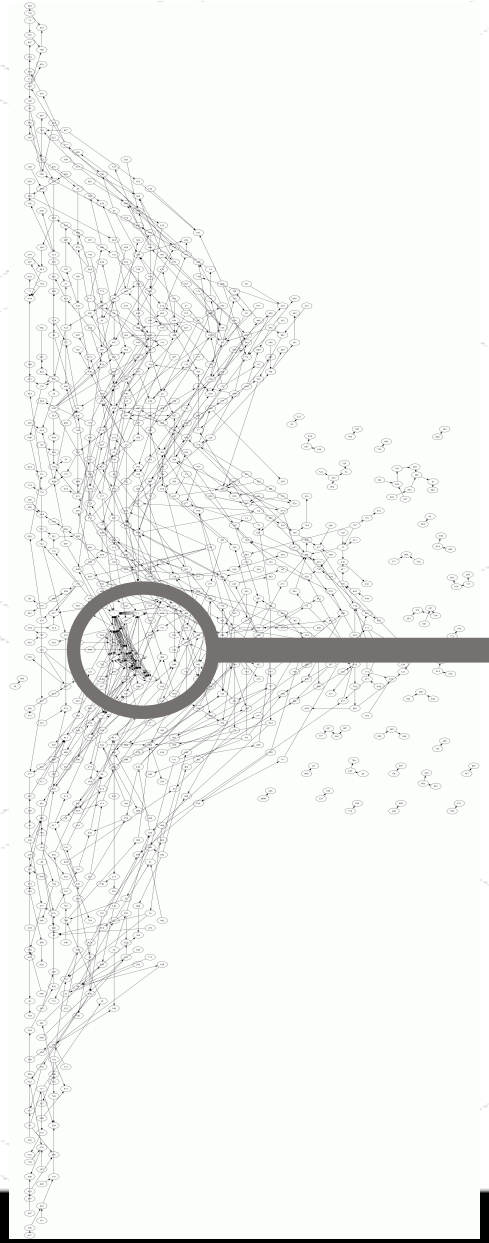
Graphviz has been installed on the Win10 VM. Use the data sets provided on WebCMS (1000 example.xlsx) to explore the different kind of visualisations.

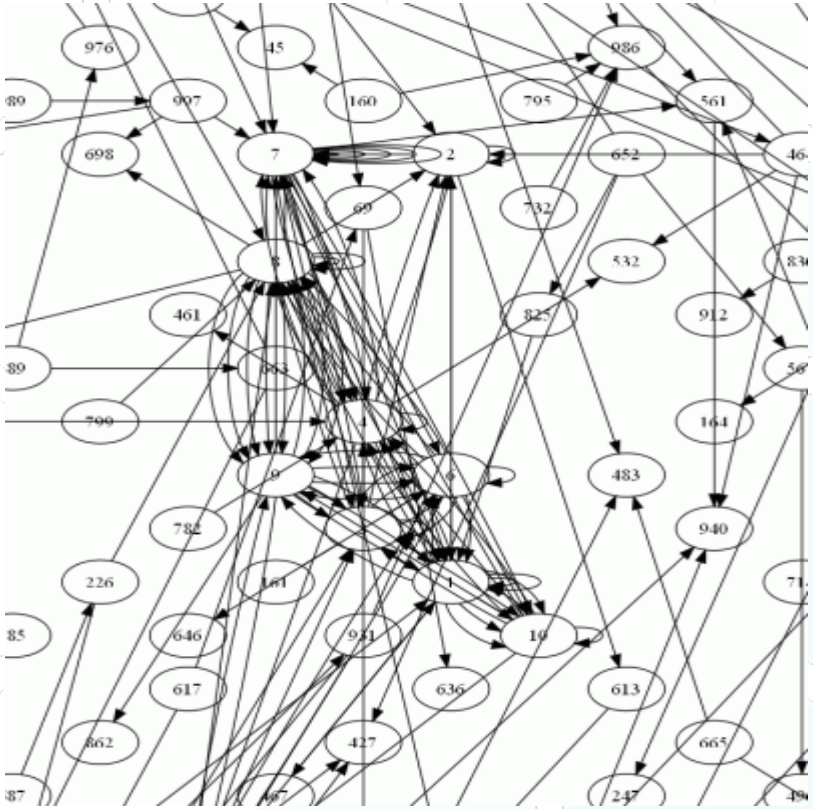
https://github.com/log2timeline/plaso

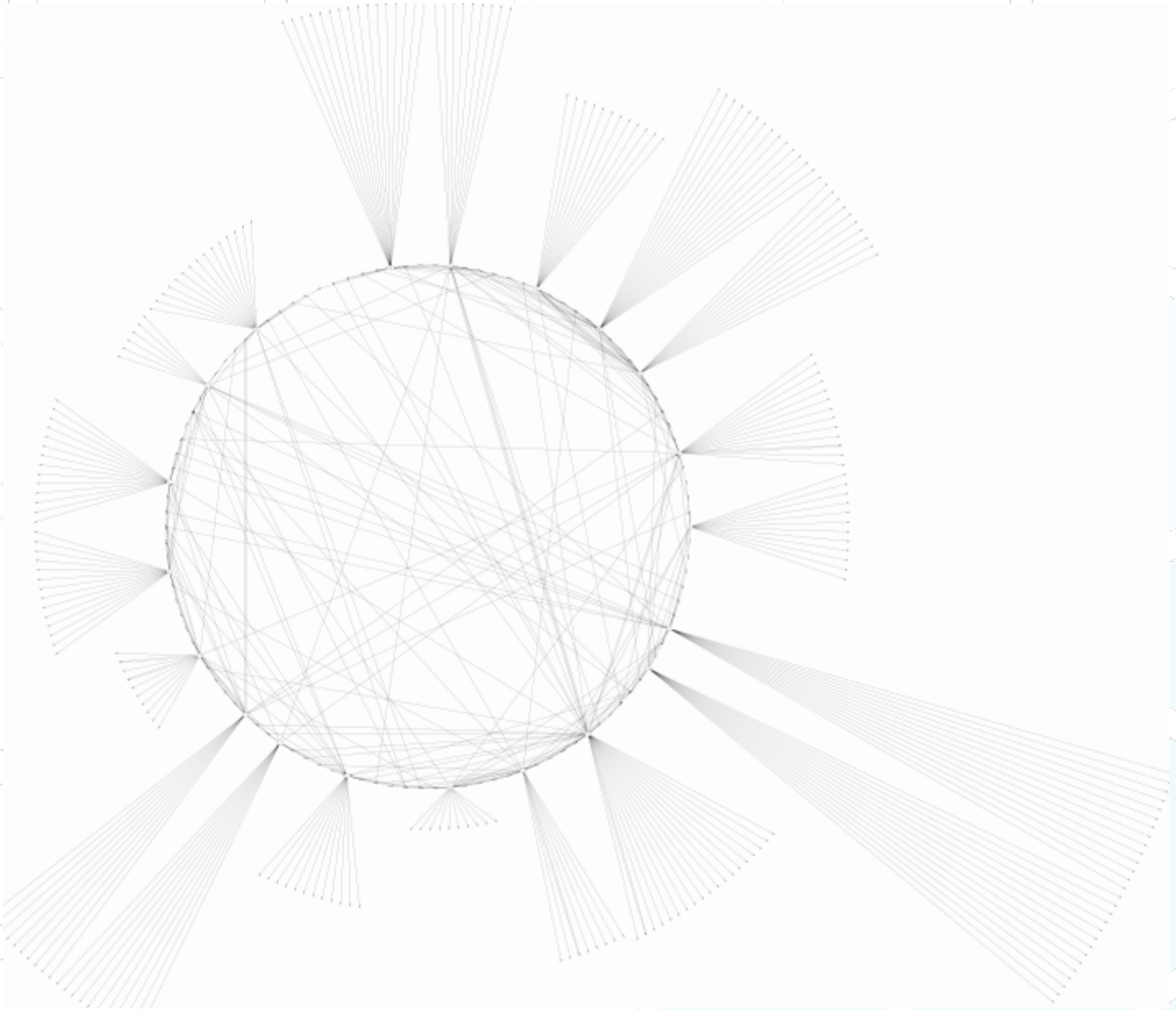
https://www.graphviz.org/

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	From	To	From	To	From	To	From	To	From	To	From	To	From	To	From	To	From	To	From	To	From	To	From	To
2	391	670	968	761	143	477	857	317	078	396	511	305	517	836	642	241	805	810	696	097	875	057	486	082
3	986	845	763	015	576	160	822	913	735	892	930	573	234	338	147	021	714	362	412	672	187	670	842	661
4	220	713	734	594	264	039	293	285	659	739	137	568	428	953	927	210	367	138	630	983	656	853	374	327
5	816	370	112	782	483	318	721	146	634	336	748	878	619	510	798	431	260	860	466	986	784	740	098	934
6	478	314	778	857	445	482	471	135	153	016	845	459	735	675	561	103	435	933	072	632	315	986	954	517
7	218	614	576	274	496	534	857	841	419	862	637	901	887	593	155	396	007	644	141	239	934	545	780	288
8	453	050	011	684	817	890	959	970	195	876	354	090	654	432	540	943	318	724	572	988	984	741	517	858
9	604	269	980	700	112	500	935	774	368	980	828	547	240	301	552	907	499	052	445	351	760	099	004	841
10	377	879	057	442	678	878	091	171	860	878	689	339	453	662	848	831	805	549	535	753	917	068	868	272
11	009	001	005	004	005	006	007	003	002	010	005	005	006	005	009	010	005	010	010	008	008	009	010	009
12	420	403	588	825	493	983	317	018	436	103	932	737	412	763	244	671	820	480	001	112	681	466	088	426
13	498	550	320	941	934	307	642	576	294	818	036	359	536	192	917	806	301	219	183	309	894	920	710	314
14	361	785	107	743	894	687	115	716	488	685	502	717	129	609	024	752	139	855	862	018	485	151	899	701
15	099	942	535	124	553	249	999	055	334	484	834	384	692	014	091	331	287	256	805	956	784	533	961	489
16	872	631	574	978	755	665	432	749	041	477	977	034	545	139	282	145	920	411	648	228	331	443	274	606
17	257	485	931	201	575	644	752	817	454	093	952	585	012	159	935	736	926	769	086	839	101	568	268	615
18	350	483	182	777	132	311	895	932	713	896	091	933	431	392	786	433	330	806	941	233	482	499	374	585
19	826	061	195	561	831	357	181	745	250	539	041	137	203	836	502	028	244	367	608	916	536	306	899	155
20	331	683	868	335	908	123	148	326	863	944	640	235	209	783	796	136	718	245	157	715	167	676	329	969
21	005	006	001	006	008	005	008	006	005	006	001	007	009	008	004	006	004	005	004	009	004	009	008	001
22	119	192	067	008	517	936	726	100	815	526	794	187	402	604	273	518	108	237	058	427	631	341	277	689
23	793	644	406	595	245	486	807	790	234	502	197	861	040	682	217	839	728	1000	594	231	583	279	946	563
24	189	315	471	785	544	629	413	263	743	016	702	724	198	971	859	808	064	400	072	922	656	243	195	752
25	036	527	517	244	928	561	339	118	626	568	433	716	232	743	918	302	547	097	187	465	362	642	179	378
26	098	629	738	683	463	903	562	001	690	003	159	796	748	020	057	441	149	868	807	293	145	247	314	629
27	589	665	928	928	819	555	605	085	557	912	512	074	428	120	612	844	936	122	339	701	867	167	111	879
28	916	229	736	833	698	277	164	594	632	706	891	675	554	296	833	068	555	004	988	911	825	763	704	658
29	396	533	712	944	988	597	021	663	374	131	611	235	872	401	866	390	408	592	097	038	821	700	531	867
30	234	698	719	583	645	997	901	028	530	447	738	835	612	751	254	265	328	466	309	264	141	698	367	002
31	003	004	005	001	009	002	002	008	005	005	002	008	002	001	008	002	004	005	004	008	007	003	008	009
32	170	454	718	505	926	502	916	183	891	756	560	591	943	728	746	166	890	290	443	835	282	362	402	702
33	359	151	509	027	176	782	750	338	110	707	209	140	581	986	207	929	524	786	694	916	217	983	626	375
34	231	815	003	371	667	287	608	658	222	986	930	801	939	245	603	394	262	548	463	491	521	611	887	441
35	784	221	141	176	831	125	233	583	076	587	073	649	586	101	700	664	153	040	013	847	896	818	730	089
36	077	524	797	213	602	643	702	304	868	876	492	597	838	589	564	935	543	872	311	656	613	045	797	574
37	684	848	841	328	422	710	362	003	789	361	215	107	388	513	664	244	363	746	025	281	042	401	616	618
38	396	504	508	359	544	203	599	589	425	856	717	256	802	251	467	614	152	805	749	665	960	896	350	682
39	245	124	114	596	194	802	237	722	399	960	017	895	664	431	636	783	947	811	526	884	576	466	517	182
40	347	281	694	563	715	959	230	970	259	408	248	467	082	579	805	855	440	702	106	218	515	493	868	114
41	007	001	004	003	010	004	003	002	002	010	005	003	006	007	003	002	007	005	001	005	001	007	006	009
42	883	546	683	477	021	318	070	174	598	606	285	872	119	843	223	570	581	014	549	117	220	318	867	257
43	248	015	001	791	353	037	456	393	611	867	685	770	790	625	853	765	673	104	377	151	639	206	774	639
44	883	682	053	734	727	520	130	017	057	225	228	994	243	118	269	491	688	314	533	830	384	500	113	057
45	794	260	191	611	814	026	944	887	732	875	227	873	341	822	855	966	546	025	763	119	700	099	338	928


464
2
1
10
467
281
9
82
507
177
862
7
746
984
181
3
244
782
263
512
233
658
646
415
4
171
214
532
650
161
288
917
5
461
545
6
211
274
482
475
799
103
633
284
718
84
665
8



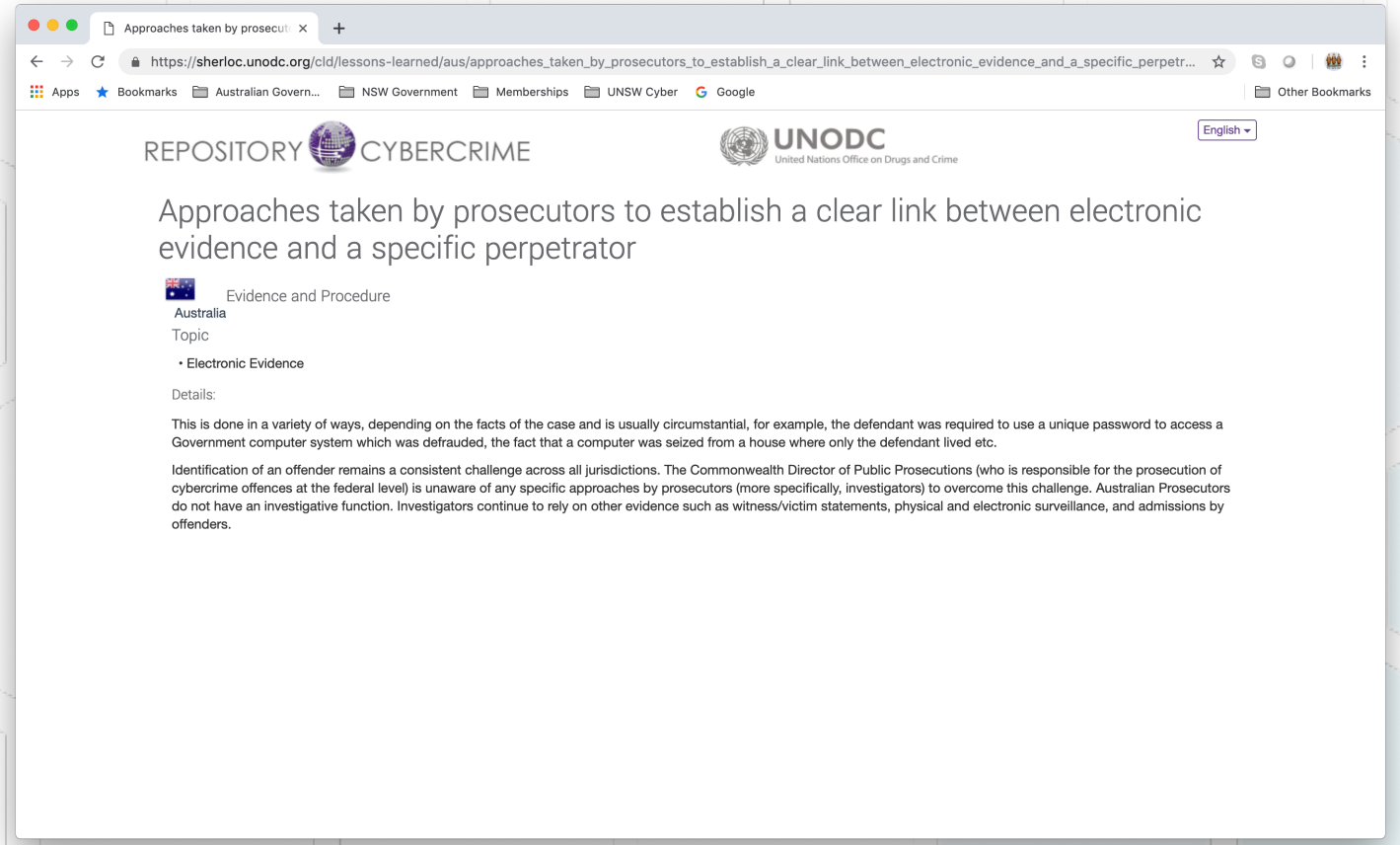

976
45
986
907
160
795
561
698
7
2
652
732
532
461
825
912
799
164
483
782
940
226
646
934
617
636
613
862
427
665



Translating IP address to person or geographical address

- For operational or intelligence purposes, it may be good enough to identify an IP address or address range
  - Block the address
- For forensic purposes, it is almost always necessary to link the IP address to a person or entity
  - There may be several steps e.g. link to address and then to person at that address
  - Starting point is IP address date and time
  - May rely on circumstantial evidence e.g. the person is using the phone

UN Office on Drugs and Crime - Australia



https://sherloc.unodc.org/cld/lessons-learned/aus/approaches_taken_by_prosecutors_to_establish_a_clear_link_between_electronic_evidence_and_a_specific_perpetrator.html?&tmpl=cyb

Need to understand DNS and Internet registries

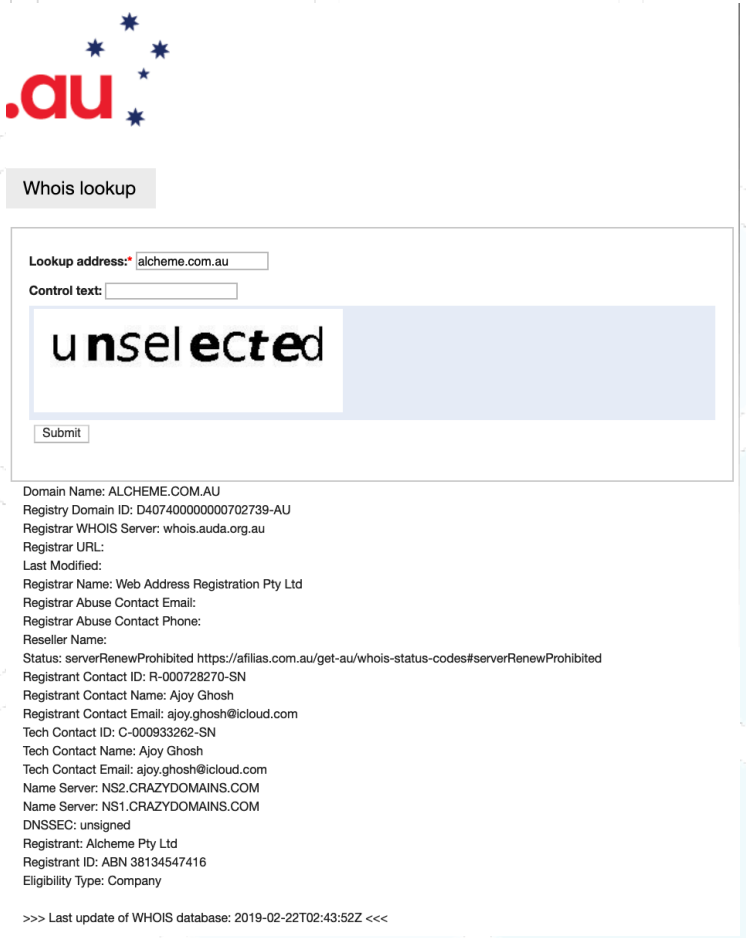
- Internet Assigned Numbers Authority (IANA)
- Regional internet registries (RIR)
- National/Local internet registry
  - Assigned a block by RIR and responsible for allocating addresses within the block
- auDA[1] is the local registry for Australia and has delegated registration to accredited registrars[2]

Registry	Geographic Region
AFRINIC	Africa, portions of the Indian Ocean
APNIC	Portions of Asia, portions of Oceania
ARIN	Canada, many Caribbean and North Atlantic islands, and the United States
LACNIC	Latin America, portions of the Caribbean
RIPE NCC	Europe, the Middle East, Central Asia

1. See https://www.auda.org.au/
2. List of registrars is here: https://www.auda.org.au/industry-information/registrars/

Whois and IP lookups

- Use authoritative data sources
  - auDA provided Whois[1] for
    - asn.au
    - com.au
    - edu.au
    - gov.au
    - id.au
    - net.au
    - org.au
- IP lookups using registered Name Server (if possible)



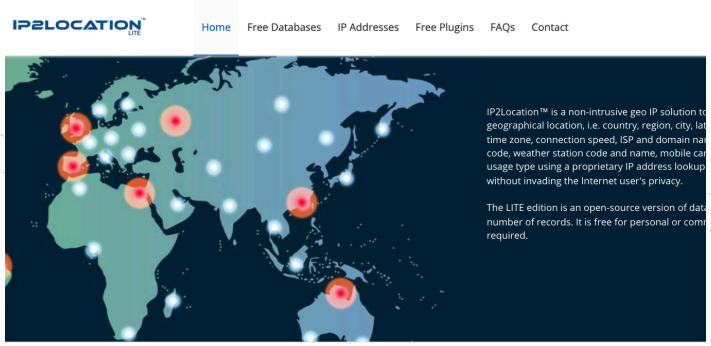
1. https://whois.auda.org.au/

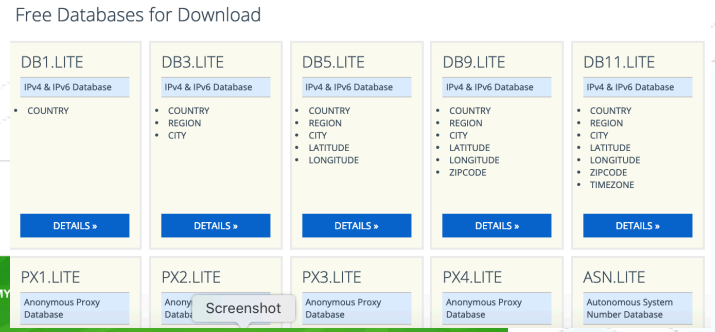
IP address geolocation tools

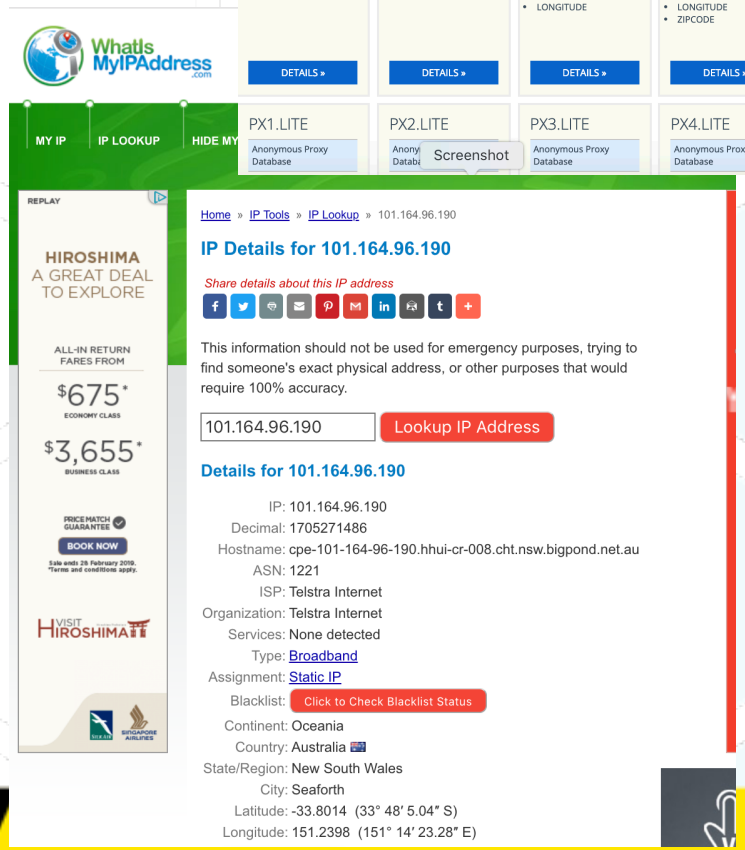
- Use IP geolocation databases
  - Commercial and free
- WhatisMyIPAddress[1] and IP2location LITE[2] are commonly used free resources

ACTIVITY for home

- Read the APNIC FAQ on geolocation[3] that is also provided in the readings







1. https://whatismyipaddress.com/
2. https://lite.ip2location.com/
3. https://www.apnic.net/get-ip/faqs/geolocation/

Mandatory Data Retention[1]

- 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

- Access for 15 LEAs
  - A wide range of government agencies have applied for and been granted access[2]

ABC NEWS

Just In | Politics | World | Business | Sport | Science | Health | Arts | Analysis

Print | Email | Facebook | Twitter | More

List of agencies applying for metadata access without warrant released by Government

By political reporter Stephanie Anderson

Updated 18 Jan 2016, 3:54pm

The Federal Government has released a list of more than 60 federal, state and local government agencies that have applied to access metadata.

The list released under Freedom of Information laws showed agencies that have sought to access telecommunications data without a warrant.

As well as numerous federal departments, requests were also made by the Bankstown City Council, the National Measurement Institute and Greyhound Racing Victoria.

Organisations classed as "criminal law-enforcement agencies" already have access to metadata under the Federal Government's data retention bill, passed last year.

RELATED STORY: ISPs 'still waiting' on Government funding for new data laws

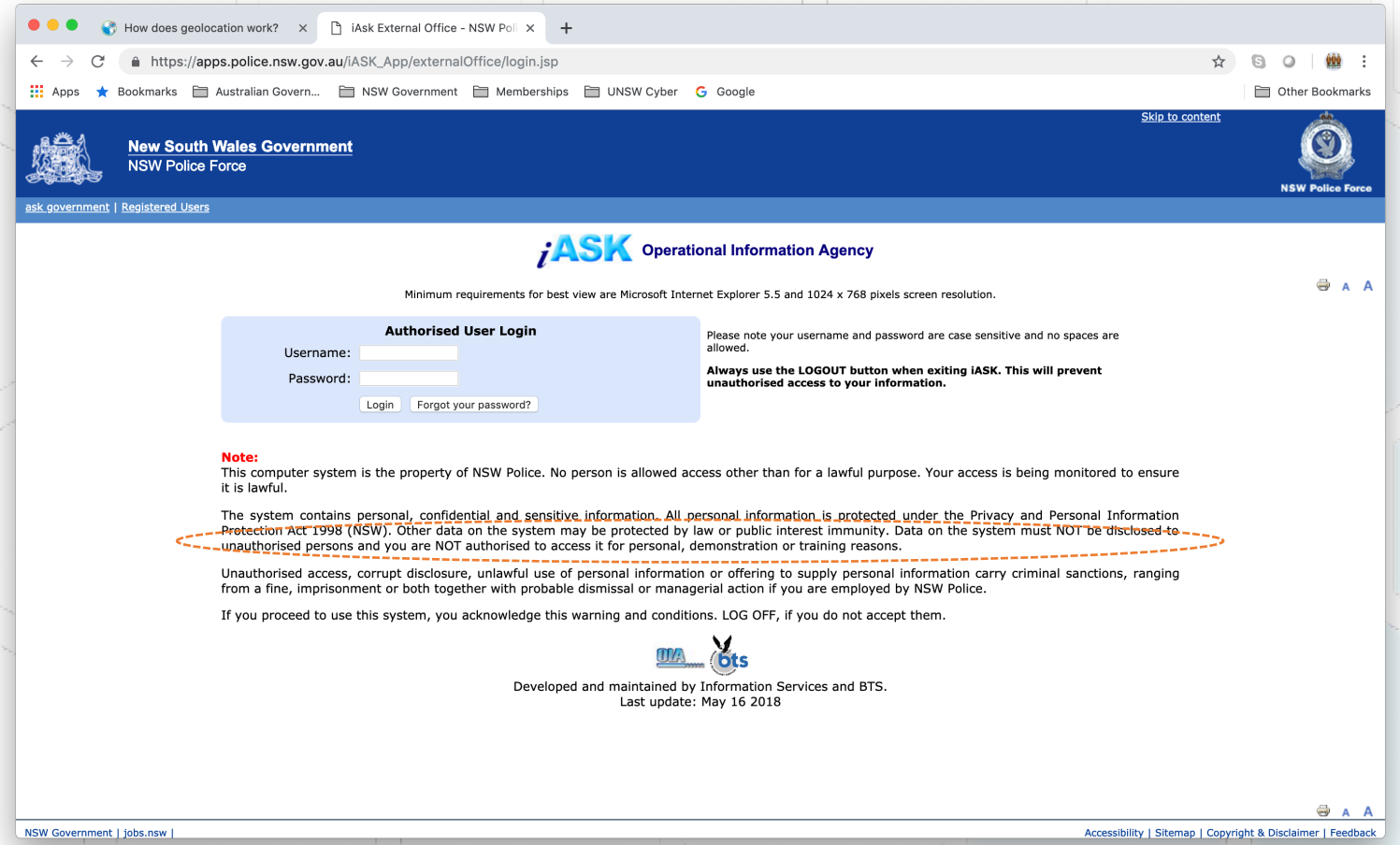
RELATED STORY: 'Scarily accurate': What you found in our reporter's metadata

RELATED STORY: How your phone tracks your every move

What is metadata?

1. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
2. https://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836 that also has a document with a list of 60 agencies granted access

Law enforcement requests e.g. NSW Police iASK



See https://apps.police.nsw.gov.au/iASK_App/externalOffice/login.jsp

Court order against service provider or company

- Need to understand in they are a “carriage” or “content” service[1]
- These can be an expensive, slow and frustrating activity
- Some providers are overseas (for service of orders) and will demand orders from a Court in their jurisdiction
  - Australian Court will probably have jurisdiction, but it is a question of efficacy
- Many make it difficult to obtain details of their Australian office and how to serve orders
- It is not uncommon for an order to be returned claiming the required information was not provided
  - Some providers assert their own requirements on the form of request
- Increasingly common for Telcos and ISPs to respond that the requested data is part of the MDR data set and can only be provided under that scheme
- Even when they don’t resist they will take time to respond
  - 3 months is typical even when the data is available with 1-3 days for a law enforcement request

The Joint Cyber Security Centres are helping to smooth the process for those of you who are JCSC participants

How many requests do we receive each year?

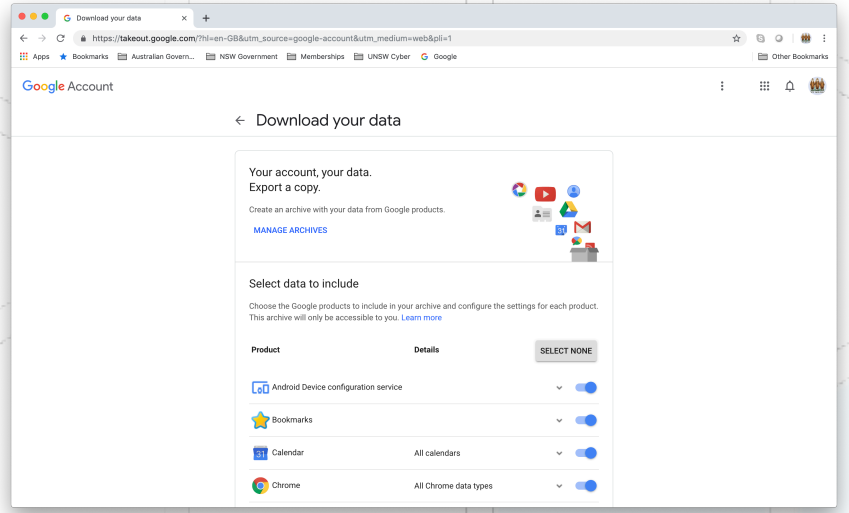
Between 1 July 2017 and 30 June 2018, Telstra responded to 74,089 requests for customer information.

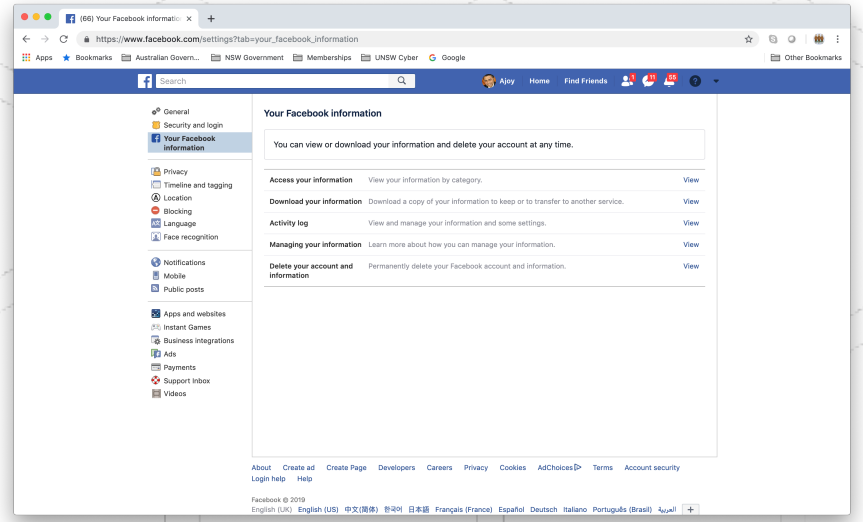
- 66,671 involved providing customer information
- 4,214 involved life-threatening situations and emergency calls
- 370 were copyright – DNS Blocking requests
- 2,329 were warrants for interception or access to stored communications
- 505 were court orders

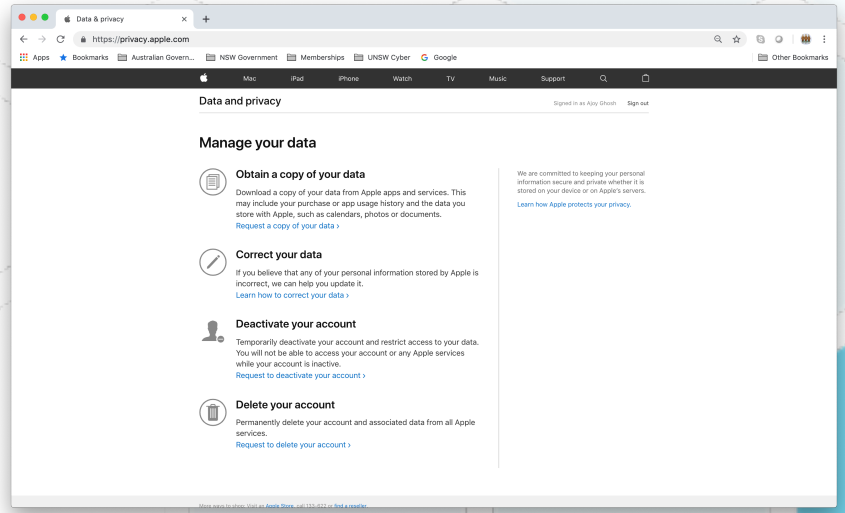
1. See Telecommunications Act §14 - §16
2. Excerpt from Telstra – our legal obligation to provide information see https://www.telstra.com.au/consumer-advice/your-information/law-enforcement

Download my data

- Available for:
  - Google
    - Account
  - Apple iCloud
    - Privacy portal
  - Facebook
    - Download your information
  - Many others







PCAP and Netflow

- Core protocols used for network forensic capture and analysis.

- PCAP and PCAPNG (PCAP next generation) is the format used by many tools
  - Libpcap became de-facto standard for Unix/Linux
  - TCPDump, Windump, Snort, Wireshark etc
  - Many commercial tools

- Netflow original introduced by CISCO. Equivalent protocols now adopted by most manufacturers, using V4 for IPv4 and V9 for IPv6

Explore PCAP and Netflow in tomorrows tutorial/labs

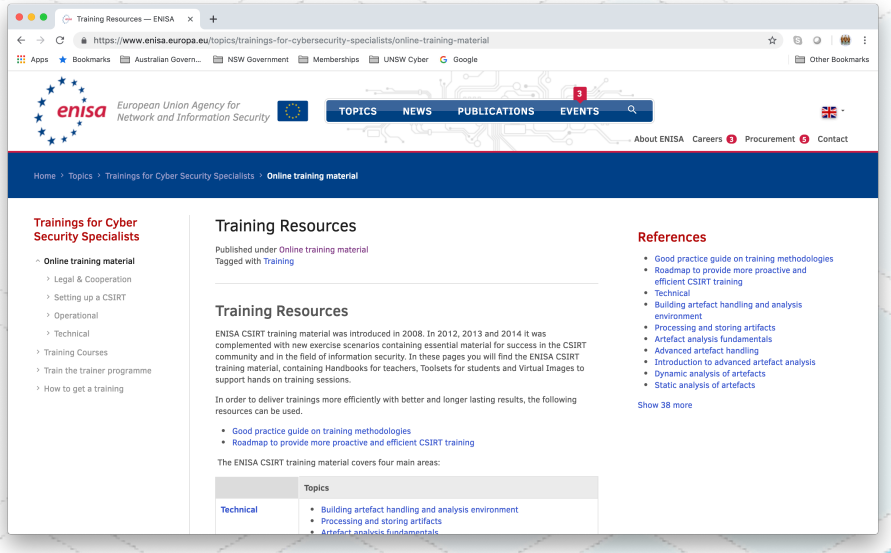
Short break – 5 mins

And then Week 6 part 3

Tutorial/lab – spread across weeks 6 and 7

- Use training scenario from European Union Agency for Network and Information Security (ENISA)

- Student manual on WebCMS and virtual machine on external hard disk drive
- Perform selected ENISA technical scenarios:
  - Task 2: Dabber attack scenario (p11)
  - Task 5: Netflow analysis (p19)



See https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material