



**security
engineering
capability**



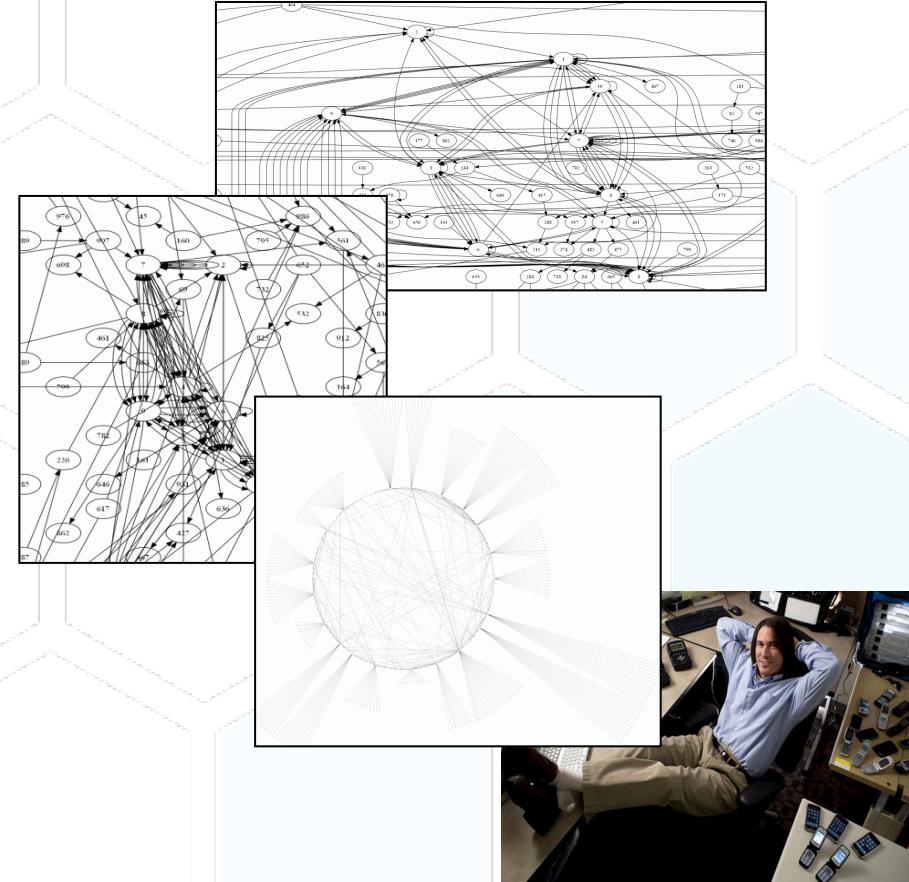
COMP6445 – Digital Forensics

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 activities¹

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>

The Sydney Morning Herald



Job hunting?
What the best employers are looking for

The new graduate job seeker's guide to the top 100 employers

[FIND OUT MORE](#)

Advertisement

TECHNOLOGY GOVERNMENT IT

NSW Police use hacking software to spy on computers and smartphones: WikiLeaks data

By Ben Grubb
Updated September 15, 2014 – 4:35pm, first published at 2:28pm

NSW Police are using sophisticated hacking software to spy on smartphones and computers during criminal investigations, according to documents published by WikiLeaks on Monday.

FinFisher, also known as FinSpy, is surveillance software sold by German company Gamma International. The software is typically used by intelligence and policing agencies to break into computers and mobiles and can secretly log keystrokes and take screenshots.



Martin Muench, managing director of Gamma International, poses for a photo in 2012. BLOOMBERG

It can also remotely capture Skype and instant messenger conversations and take control of

ABC NEWS

Just In Politics World Business Sport Science Health Arts Analysis

Print Email Facebook Twitter More

Spyware for sale: Hacking Team leaks show Australian companies scrambling to cash in on Government surveillance contracts

7.30 By the National Reporting Team's Lisa Main and Conor Duffy
Updated 29 Jul 2015, 8:45am

At least four Australian companies have tried to sell a range of controversial spyware and surveillance tools to Australian law enforcement agencies as well as foreign governments, according to emails revealed by WikiLeaks.

The sophisticated spyware has been developed by controversial Italian company Hacking Team, which recently came under criticism for its links to repressive regimes.

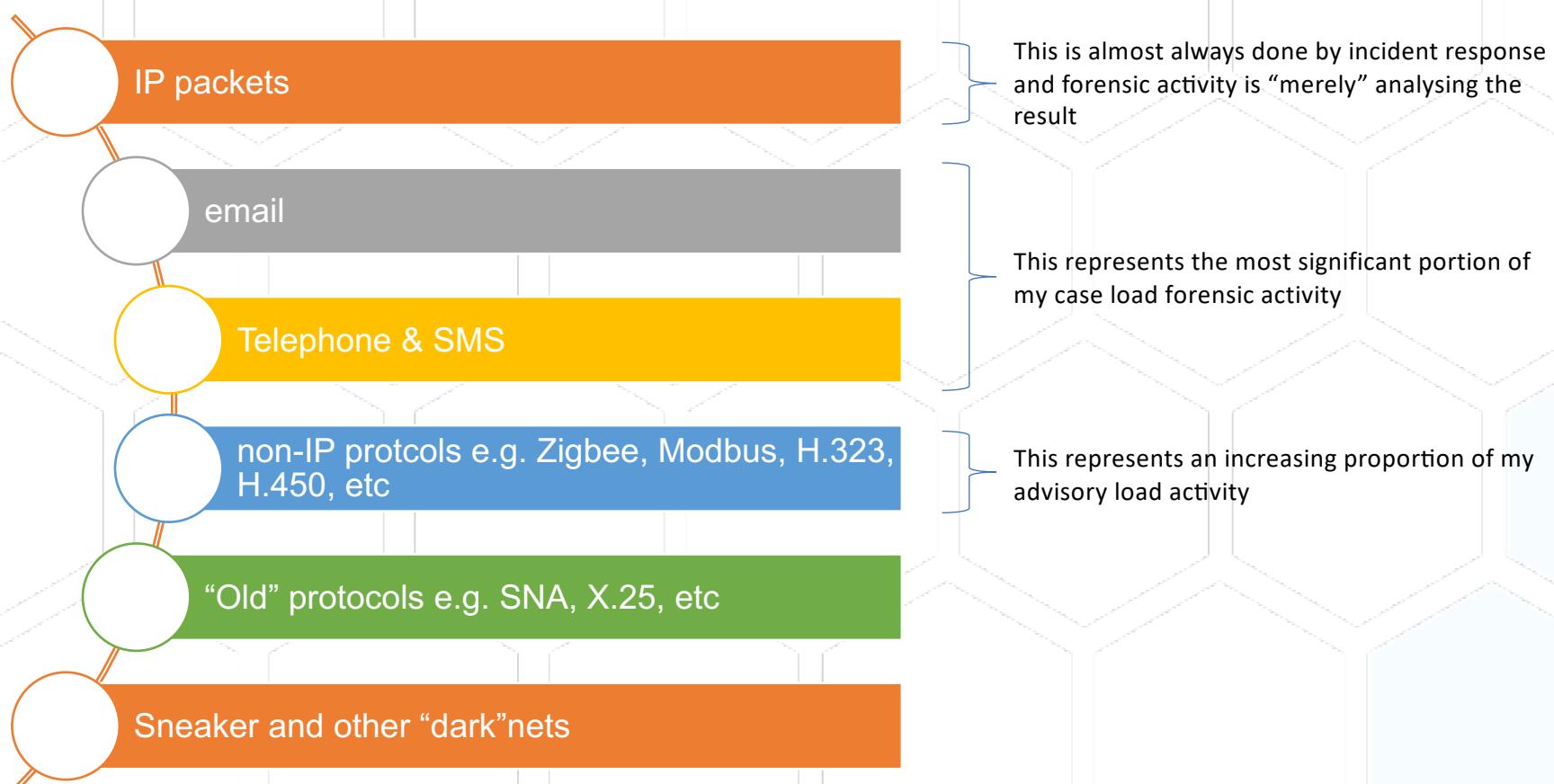
Earlier this month Hacking Team's inner workings were revealed after the company itself was hacked and thousands of emails were published by WikiLeaks.

The trove of emails exposed the secretive and lucrative dealings of the private surveillance industry.

An investigation by the ABC revealed Australian companies have been acting as middle-men, dealing with Hacking Team on the one hand, and agencies such as the Australian Federal Police, Defence and Indonesian intelligence on the other.

VIDEO: Australian police and Defence Force used infamous Hacking Team, WikiLeaks reveals (7.30)

Common interactions to be analysed



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>

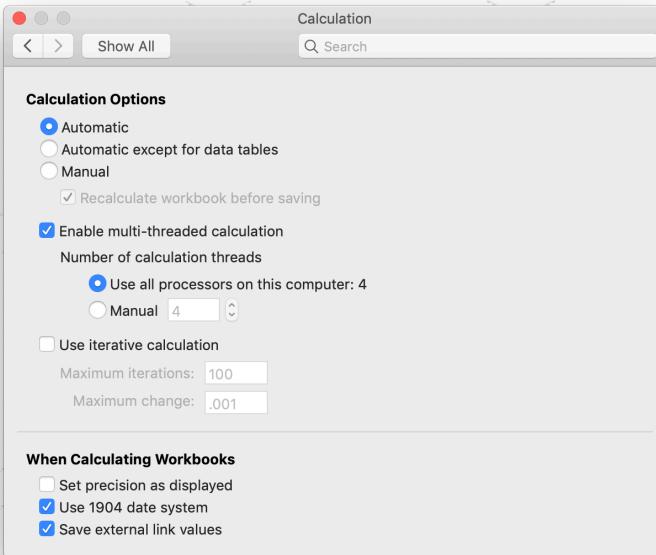
Time

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
 - Log2timeline¹ produced tagged data. Useful for email, browsing history, etc
 - Graphviz² 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



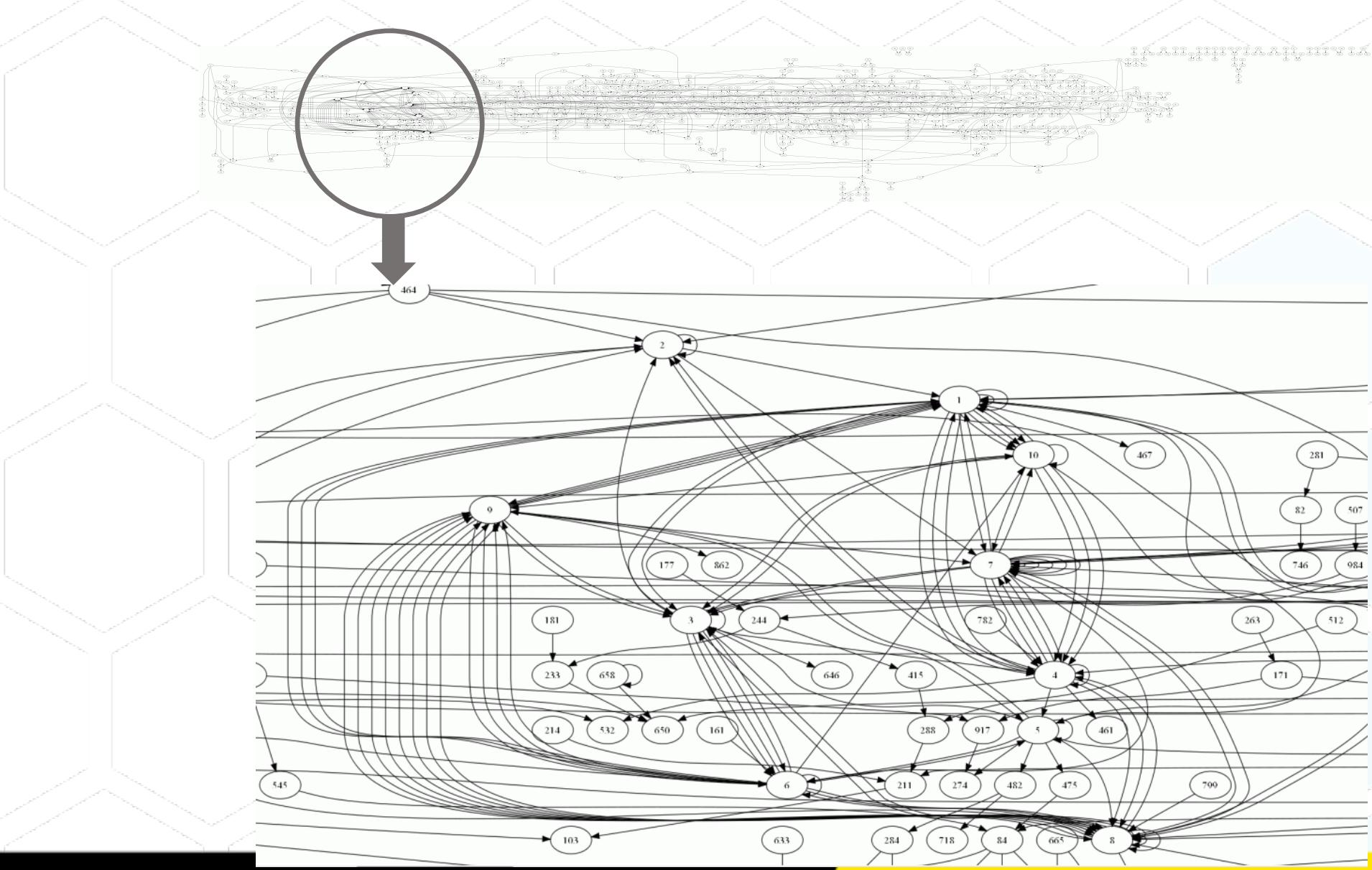
ACTIVITY for home

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.

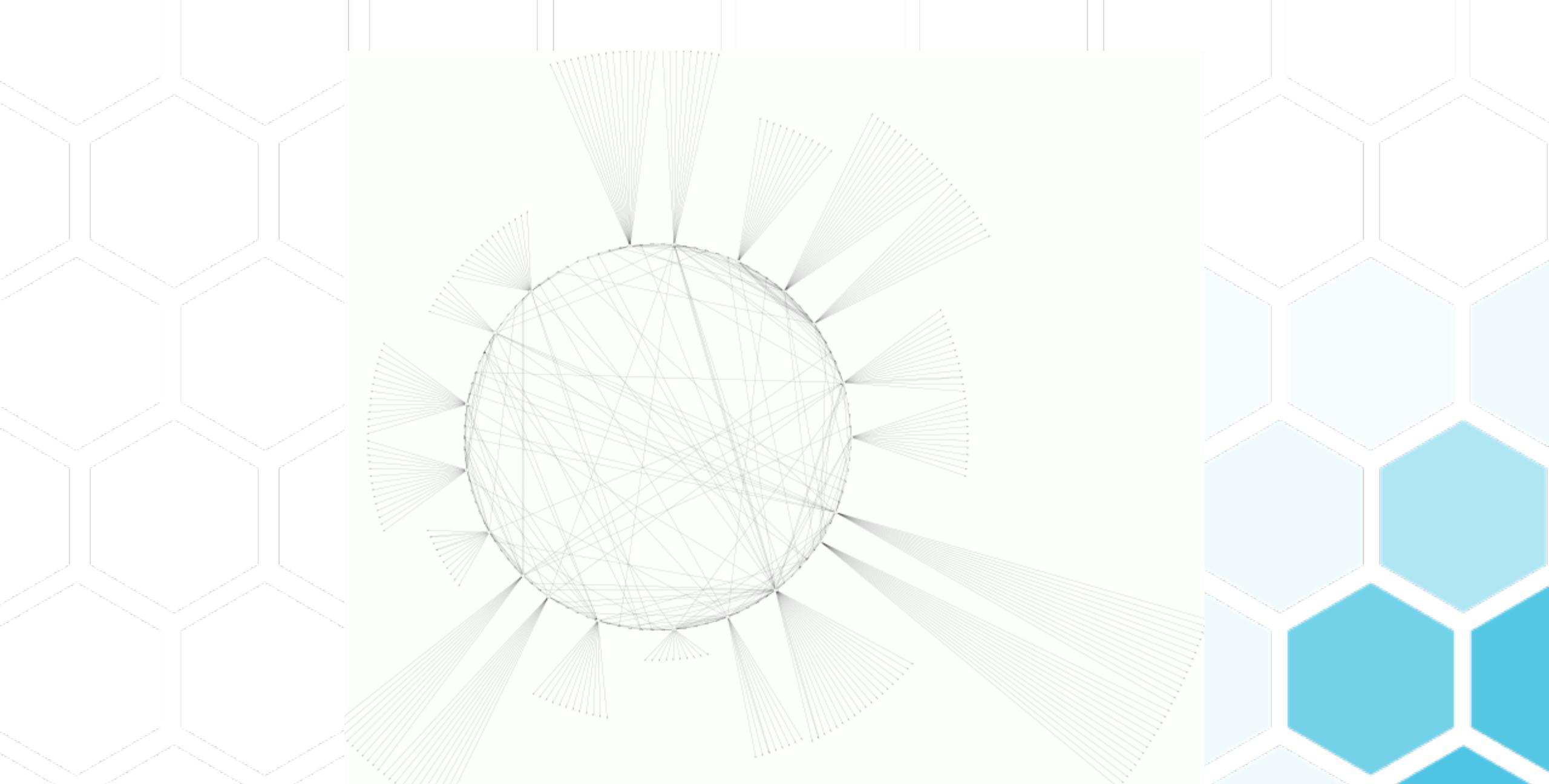
<https://github.com/log2timeline/plaso>

<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	
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	963
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	899	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	656
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	284	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	581	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	684	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







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

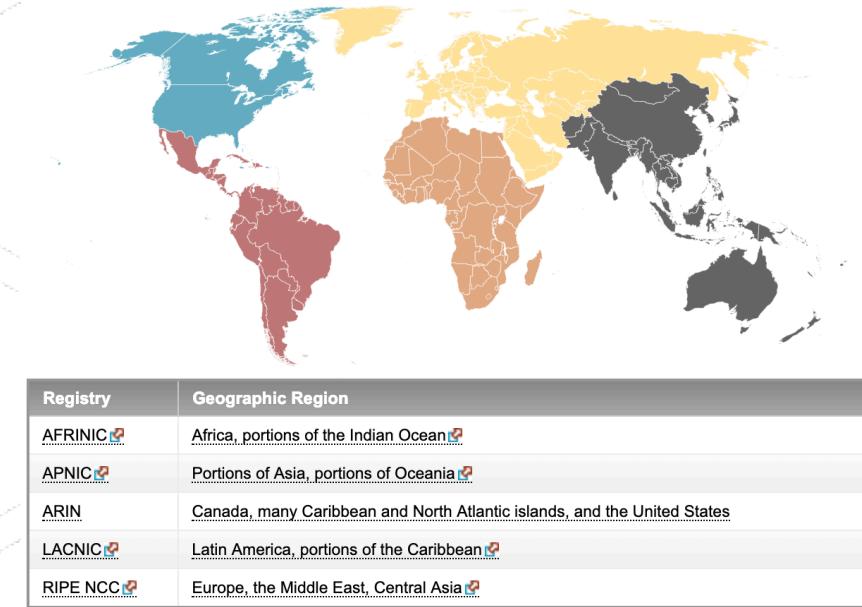
The screenshot shows a web browser window with the following details:

- Title Bar:** Approaches taken by prosecutors to establish a clear link between electronic evidence and a specific perpetrator
- Address Bar:** 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
- Toolbar:** Includes icons for Apps, Bookmarks, Australian Government, NSW Government, Memberships, UNSW Cyber, Google, and Other Bookmarks.
- Header:** REPOSITORY CYBERCRIME (with a globe icon) and UNODC United Nations Office on Drugs and Crime (with a UN emblem).
- Language:** English
- Content:**
 - Evidence and Procedure:** Australia
 - Topic:** Electronic Evidence
 - Details:** This is done in a variety of ways, depending on the facts of the case and is usually circumstantial, for example, the defendant was required to use a unique password to access a Government computer system which was defrauded, the fact that a computer was seized from a house where only the defendant lived etc.
 - Text:** Identification of an offender remains a consistent challenge across all jurisdictions. The Commonwealth Director of Public Prosecutions (who is responsible for the prosecution of cybercrime offences at the federal level) is unaware of any specific approaches by prosecutors (more specifically, investigators) to overcome this challenge. Australian Prosecutors do not have an investigative function. Investigators continue to rely on other evidence such as witness/victim statements, physical and electronic surveillance, and admissions by offenders.

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
- auDA¹ is the local registry for Australia and has delegated registration to accredited registrars²



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 Whois¹ 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/>

The screenshot shows a web form titled "Whois lookup". The "Lookup address:" field contains "alcheme.com.au". Below the form, the word "unselected" is displayed in large, bold, black letters. A "Submit" button is located below the form fields. To the right of the form, detailed WHOIS information is listed:

Domain Name: ALCHEME.COM.AU
Registry Domain ID: D40740000000702739-AU
Registrar WHOIS Server: whois.auda.org.au
Registrar URL:
Last Modified:
Registrar Name: Web Address Registration Pty Ltd
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller Name:
Status: serverRenewProhibited https://afilias.com.au/get-au/whois-status-codes#serverRenewProhibited
Registrant Contact ID: R-000728270-SN
Registrant Contact Name: Ajoy Ghosh
Registrant Contact Email: ajoy.ghosh@icloud.com
Tech Contact ID: C-000933262-SN
Tech Contact Name: Ajoy Ghosh
Tech Contact Email: ajoy.ghosh@icloud.com
Name Server: NS2.CRAZYDOMAINS.COM
Name Server: NS1.CRAZYDOMAINS.COM
DNSSEC: unsigned
Registrant: Alcheme Pty Ltd
Registrant ID: ABN 38134547416
Eligibility Type: Company

>>> Last update of WHOIS database: 2019-02-22T02:43:52Z <<<

IP address geolocation tools

- Use IP geolocation databases
 - Commercial and free
- WhatisMyIPAddress¹ and IP2location LITE² are commonly used free resources

ACTIVITY for home

- Read the APNIC FAQ on geolocation³ 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/>



Free Databases for Download

DB1.LITE IPv4 & IPv6 Database	• COUNTRY	DB2.LITE IPv4 & IPv6 Database	• COUNTRY	DB3.LITE IPv4 & IPv6 Database	• COUNTRY	DB4.LITE IPv4 & IPv6 Database	• COUNTRY	DB5.LITE IPv4 & IPv6 Database	• COUNTRY	DB6.LITE IPv4 & IPv6 Database	• COUNTRY	DB7.LITE IPv4 & IPv6 Database	• COUNTRY	DB8.LITE IPv4 & IPv6 Database	• COUNTRY	DB9.LITE IPv4 & IPv6 Database	• COUNTRY	DB10.LITE IPv4 & IPv6 Database	• COUNTRY	DB11.LITE IPv4 & IPv6 Database	• COUNTRY
DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »		DETAILS »	
PX1.LITE Anonymous Proxy Database		PX2.LITE Anonymous Proxy Database		PX3.LITE Anonymous Proxy Database		PX4.LITE Anonymous Proxy Database		ASN.LITE Autonomous System Number Database													
Anony Data		Screenshot		Anony Data		Screenshot		Anony Data		Screenshot		Anony Data		Screenshot		Anony Data		Screenshot		Anony Data	

The screenshot shows two main sections. On the left, there's a flight search interface for a flight from Hiroshima to Sydney. It displays a green banner for "HIROSHIMA A GREAT DEAL TO EXPLORE", flight details (ALL-IN RETURN FARES FROM \$675* ECONOMY CLASS and \$3,655* BUSINESS CLASS), and a "BOOK NOW" button. On the right, there's a detailed IP lookup result for the IP address 101.164.96.190. The result includes the IP address itself, a "Lookup IP Address" button, and a "Details for 101.164.96.190" section. This section provides extensive information about the IP, including its decimal value (1705271486), hostname (cpe-101-164-96-190.hhui-cr-008.cht.nsw.bigpond.net.au), ASN (1221), ISP (Telstra Internet), Organization (Telstra Internet), Services (None detected), Type (Broadband), Assignment (Static IP), and Blacklist status (Click to Check Blacklist Status). It also lists the continent (Oceania), country (Australia), state/province (New South Wales), city (Seaforth), latitude (-33.8014), and longitude (151.2398).

Mandatory Data Retention¹

- 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 access²

The screenshot shows a news article from ABC News. The header reads "ABC NEWS" with a navigation bar below it containing links for "Just In", "Politics", "World", "Business", "Sport", "Science", "Health", "Arts", and "Analysis". Below the header are sharing options for "Print", "Email", "Facebook", "Twitter", and "More". The main title of the article is "List of agencies applying for metadata access without warrant released by Government". It is written by political reporter Stephanie Anderson and updated on 18 Jan 2016, 3:54pm. The article text discusses the release of a list of over 60 government agencies that have applied to access metadata. It notes that the list was released under Freedom of Information laws and includes requests from various federal departments, local councils, and other organizations. A sidebar on the right lists related stories: "ISPs 'still waiting' on Government funding for new data laws", "'Scarily accurate': What you found in our reporter's metadata", and "How your phone tracks your every move". At the bottom, there is a section titled "What is metadata?" with a small thumbnail image of a person at a computer.

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

How does geolocation work? *iAsk External Office - NSW Poli*

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

New South Wales Government
NSW Police Force

ask government | Registered Users

iASK Operational Information Agency

Minimum requirements for best view are Microsoft Internet Explorer 5.5 and 1024 x 768 pixels screen resolution.

Authorised User Login

Username:
Password:

Please note your username and password are case sensitive and no spaces are allowed.
Always use the LOGOUT button when exiting iASK. This will prevent unauthorised access to your information.

Note:
This computer system is the property of NSW Police. No person is allowed access other than for a lawful purpose. Your access is being monitored to ensure it is lawful.

The system contains personal, confidential and sensitive information. All personal information is protected under the Privacy and Personal Information Protection Act 1998 (NSW). Other data on the system may be protected by law or public interest immunity. Data on the system must NOT be disclosed to unauthorised persons and you are NOT authorised to access it for personal, demonstration or training reasons.

Unauthorised access, corrupt disclosure, unlawful use of personal information or offering to supply personal information carry criminal sanctions, ranging from a fine, imprisonment or both together with probable dismissal or managerial action if you are employed by NSW Police.

If you proceed to use this system, you acknowledge this warning and conditions. LOG OFF, if you do not accept them.

iMA bts
Developed and maintained by Information Services and BTS.
Last update: May 16 2018

NSW Government | jobs.nsw | Accessibility | Sitemap | Copyright & Disclaimer | Feedback

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

Court order against service provider or company

- Need to understand if they are a “carriage” or “content” service¹
- 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

This screenshot shows the 'Your Facebook Information' settings page. The left sidebar lists various categories of data: General, Security and login, Your Facebook Information (selected), Privacy, Timeline and tagging, Location, Language, Face recognition, Notifications, Mobile, Public posts, Apps and websites, Instant Games, Business integrations, Ads, Payments, Support inbox, and Videos. The main content area displays options for managing information: 'Access your information' (View), 'Download your information' (View), 'Activity log' (View), 'Delete your account and information' (View), and 'Managing your information' (View). At the bottom, there are links for About, Create ad, Create Page, Developers, Careers, Privacy, Cookies, AdChoices, Terms, and Account security.

This screenshot shows the 'Download your data' interface on Google's website. It features a header with the Google logo and a 'MANAGE ARCHIVES' button. Below is a section titled 'Select data to include' with a table showing products and their details. Products listed include: Android Device configuration service (Details), Bookmarks (Details), Calendar (All calendars), and Chrome (All Chrome data types). Each product has a 'SELECT' button next to it. A note at the top says 'Create an archive with your data from Google products.'

This screenshot shows the 'Data and privacy' settings page on Apple's website. The left sidebar lists four main options: Obtain a copy of your data, Correct your data, Deactivate your account, and Delete your account. Each option has a brief description and a 'Request a copy of your data', 'Learn how to correct your data', 'Request to deactivate your account', or 'Request to delete your account' link. The right side of the page includes a note about Apple's commitment to privacy and a link to learn more.

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

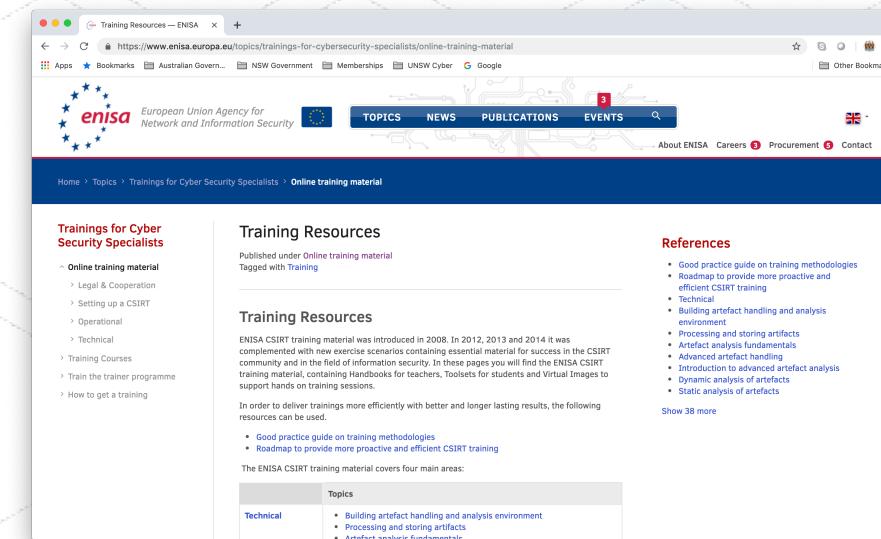
Explore PCAP and
Netflow in tomorrow's
tutorial/labs

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>