

. . . . .  
. . . . .

# COS80013

# Internet Security

Week 12

**Presented by Dr Rory Coulter**

26 May 2025



. . .  
. . .

. . . . .  
. . . . .



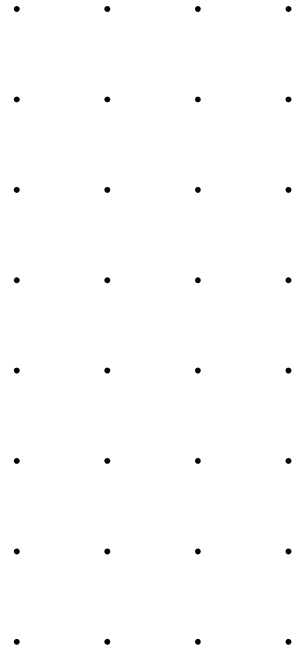
# Week 12 Class

# Assignment 2 Preparation

## Time, Logging, Memory Forensics

Overview and basic usage of each element provided

- What
- Resources
- Demonstration



# Logging

## Catchup

### Demonstration

- Exporting Windows event files
- Sysmon (DO NOT REPEAT)
  - o Deploy
  - o Live malware hash capture

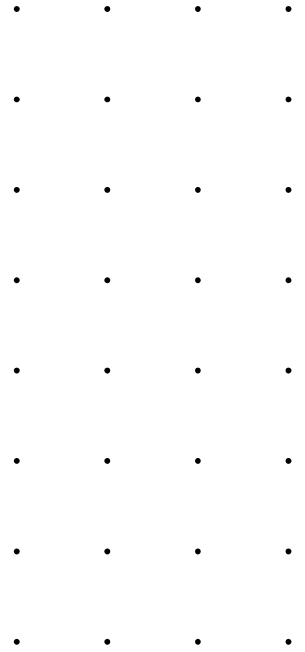


# Time

## Accounting for assets in different time zones

A common time zone

- Incidents require a timeline to understand what has occurred, placing timestamps in order
- Constructing an incident timeline allows to better understand the dwell time of the incident
- Even in Australia, assets may have different time zones between east and west
- A common time zone is needed for all assets
- UTC 0 is used as a common time zone
- All zones can be converted to this time

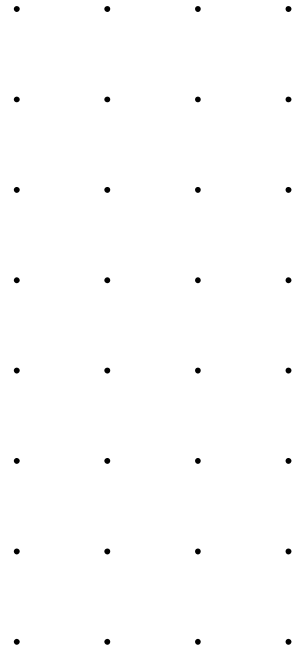


# MACB

## Each OS/Filesystem records different time information

Common between:

- M (Modified) of events and activity which has occurred
  - A (Accessed)
  - C (Changed/Meta Change)
  - B (Birth/Created)
- 
- In combination, these help produce a timeline

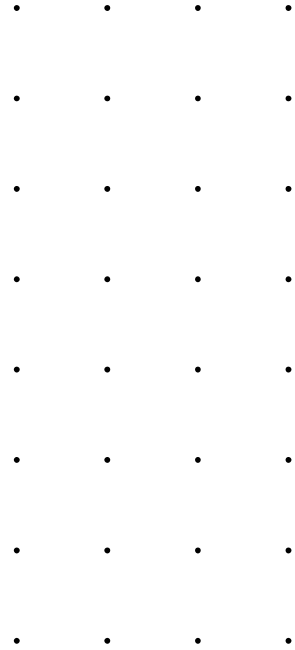


# Anti Forensics

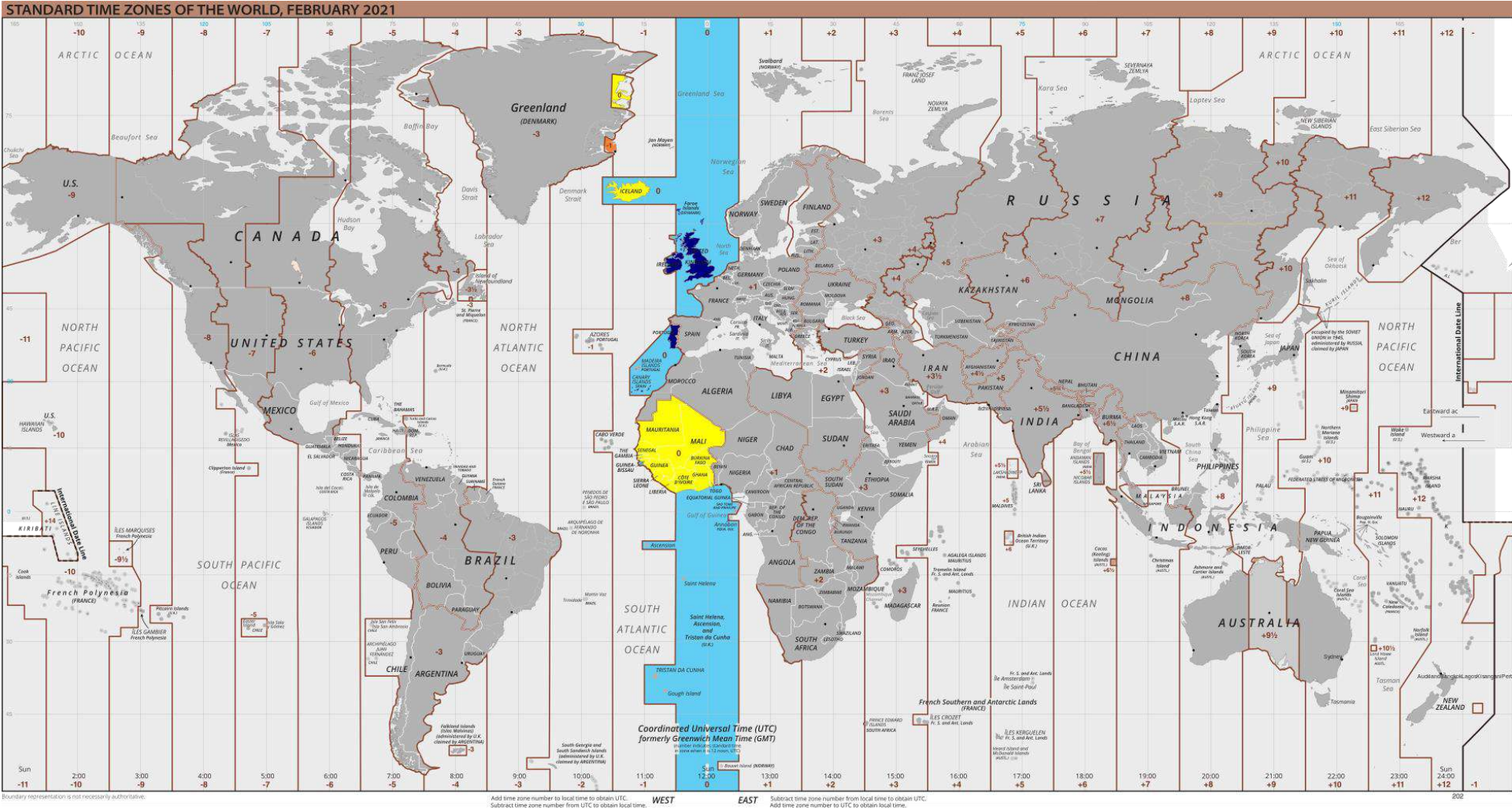
## Obstruct forensic process

Evade detection

- Time Stomp
  - o Alter timestamps
- Touch
  - o Updating timestamps
- Privacy tools
  - o Strip information from files



# UTC 0



SOURCE: By Theklan - Own work, CC0, <https://commons.wikimedia.org/w/index.php?curid=143021774>

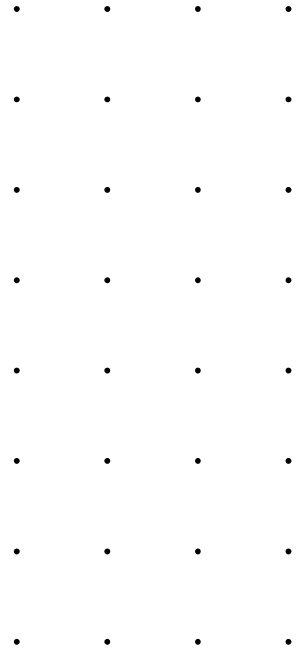


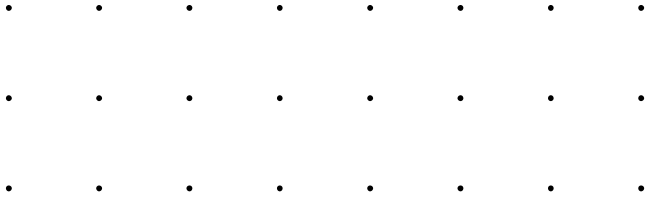
# Memory

## Demonstration

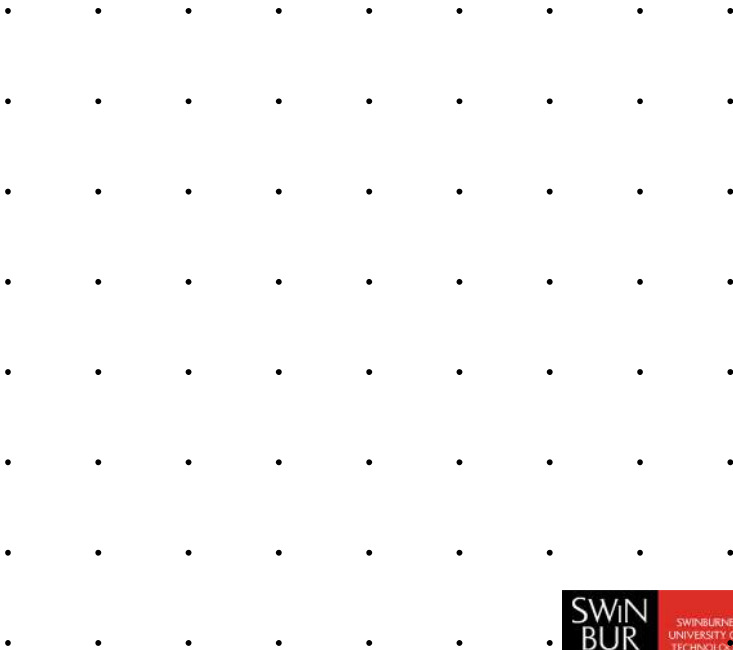
### Volatility

- File on disk
- File open in memory
- Process running
- Capture memory and analyse the above
- Profile identification





# Law



**Internet-specific laws prior to 2000 were generally not needed because most illegal activities on the Internet were covered by non-internet equivalents:**

- fraud, harassment, theft, stalking, censorship, breaking and enteringThird level

**Identity theft is an emerging problem, so new laws are being developed around the world.**

- In Australia, the Internet is predominately regulated by laws relating to media and telecommunications.
- Australian laws specific to the Internet include censorship

**Internet-specific laws prior to 2000 were generally not needed because most illegal activities on the Internet were covered by non-internet equivalents:**

- fraud, harassment, theft, stalking, censorship, breaking and enteringThird level

**Identity theft is an emerging problem, so new laws are being developed around the world.**

- In Australia, the Internet is predominately regulated by laws relating to media and telecommunications.
- Australian laws specific to the Internet include censorship

# MORE LAW

- Cyber-terrorism, (evil) hacking, DDOS and extortion are increasing.
- Internet-based espionage is flourishing.
- Technology for automated MITM of SSL is available to governments to spy on their citizens. <http://www.packetforensics.com/products.safe>
- Technology for detecting key-words (Carnivore) is spreading around the world
- USA, China, UAE, Saudi-Arabia, Swinburne?

# AUSTRALIAN LAWS

## Copyright Amendment Act (2000)

1. Fair Dealing exceptions (e.g. photocopying) for study/research/review
2. ISPs classified as common carriers – not responsible for copyright infringements (e.g. Torrents). Recently tested and confirmed (iiNet)
3. OK to re-transmit content
4. Backing up software allowed
5. Copyright extended to Internet, digital copies

# AUSTRALIAN LAWS

## Cybercrime Act (2001)

1. Terms updated to include USB disks, network storage, wifi.
2. Other terms updated
  - unauthorized access (breaking in)
  - modification
  - impairment (DOS)
3. Accidentally breaching security is not always an offence.
4. ISPs must report suspicious activities to AFP

# BUT...

## Cybercrime Act (2001)

1. ASIS and DSD granted immunity from prosecution for doing their job
2. Allowed to compel people to help them
3. Penetration testing now illegal
  - Aust. sites less hardened to attack
  - Softer targets for crackers
  - Still OK if you get written and scoped permission from the owner



# CONTINUED

## Spam Act (2003)

1. Spam must not be sent.
  - Covers e-mail, SMS, MMS, IM
  - Fax, Web pop-ups, telemarketing not prohibited.
2. Commercial mail must reveal who authorised it
3. E-mail harvesting software is illegal
4. Mailing lists created by (3) must not be used
5. Opt-in required.
6. Unsubscribe link required

# CONTINUED

## **Surveillance Devices Act (2004)**

- Police allowed to use spyware / trojans to gather evidence.
- Keyloggers
- RATs

<http://www.computerworld.com/s/article/9249352>

# CONTINUED

## Copyright law amendments (2006)

- Time-shifting now legal – record and play once
  - Lending recordings prohibited
- Backups now permitted
- Transfers to tape/disk/iPod now permitted

# CYBERCRIME LEGISLATION AMENDMENT BILL 2011

**In force 1 March 2013**

**LE agencies can request preservation of communications that carriers store, such as SMS messages, and that can be accessed only under a warrant**

- Greater co-operation with overseas LE in the investigation of cybercrime.
- Makes our laws compliant with Council of Europe Convention on Cybercrime

<http://www.smh.com.au/federal-politics/political-opinion/cyber-law-casts-the-proper-net-20110829-1jib6.html>

<http://theconversation.com/cybercrime-bill-makes-it-through-but-what-does-that-mean-for-you-8953>

# TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2015

## ISPs and telcos required to store metadata for 2 years

- Sender, recipient, time (e-mail)
- Sender, recipient, time (phone calls)
- IP (DHCP)
- Info available (on receipt of a warrant) to Aust LE, US NSA and UK GCHQ

**Not collected: organisation-wide e-mails, YouTube, Skype, Gmail, Hotmail**

<http://www.smh.com.au/federal-politics/political-news/senate-passes-controversial-metadata-laws-20150326-1m8q3v.html>

<http://www.abc.net.au/news/2015-05-08/edward-snowden-says-australias-mass-surveillance-dangerous/6456938>

# PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017

- **Starts in Feb 2018**
- **Businesses must report data breaches to customers**
- **Tell them what to do (delete, pray, update)**
- **Fines \$360k**

<https://www.itnews.com.au/news/australia-finally-has-mandatory-data-breach-notification-450923>

# FUTURE DECRYPTION LAWS (AU)

- **Force Apple, Google, Facebook to decrypt user's traffic for law enforcement agencies**
- **Hotly debated**
- **Weakens security**
- **Intended that Apple, Google, Facebook provide info; no instructions on how.**

<https://www.gizmodo.com.au/2017/07/australias-planned-decryption-law-would-weaken-cybersecurity/>

<http://theconversation.com/australias-planned-decryption-law-would-weaken-cybersecurity-81028>

## **DMCA (1998)**

- Protects copyright owners
  - Prevents fair use
- Makes bypassing copy-protection schemes (incl. encryption) illegal
  - Reverse engineering crypto is illegal
  - Studying crypto is illegal
  - Backups are illegal



## USAPatriot Act (2001)

**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**

- US Government. allowed to monitor its citizens
  - Internet taps
  - Phone taps
- No probable cause requirement
- Intelligence sharing allowed
- Voice mail reclassified as data (not a phone tap)
- Carnivore to be deployed at ISPs
  - black box which searches web traffic for keywords and reports users who type/read them

## **Cyber Security Enhancement Act (2002)**

- Police/government agencies allowed to phones/networks without a warrant
- ISPs allowed to hand over customers' private data / logs
- ISPs allowed to let police tap their networks

# US LAWS

## **2003 CAN-SPAM Act**

- Spam is legal as long as
  - Sender's name, address not false
  - Spam says it is commercial
  - Opt-out option
  - No relays, porn, brute force/dictionary
- US States prevented from introducing tougher laws
- Spam volume increased under this law

## **Cyber-crime Act (2007)**

- Conspiracy now an offence
- Minimum 10 computers before action is illegal
  - Illegal action used to be based on min \$5k damage, changed to 10 computers.
  - Protects owners of zombies
  - Exposes Bot-Herders to prosecution
- Cyber-extortion added to list of crimes

**2008**

## **CAN-SPAM updated**

- Sender better defined
- designated sender responsible for opt-out
- physical address now includes PO boxes
- Person redefined to include corporations
- Dedicated opt-out web page

## **Cybersecurity Act (2009)**

President can declare a cybersecurity emergency

- Shut down internet traffic [sic]
- Sec. of Commerce has power to access anything regardless of privacy laws.

US agencies fighting over who is in charge of cybersecurity.

# CYBERSECURITY INFORMATION SHARING BILL (2014)

- NSA having access to even more personal data
- facilitate cyber threat and attack information sharing between government and private sector companies. Must be de-identified
- The problem is that once the data are in the government's possession, there is a considerable amount of leeway in how it can be used

<http://www.nationaljournal.com/tech/a-new-cybersecurity-bill-could-give-the-nsa-even-more-data-20140627>

**[Editor's Note (Murray): One need only consider the source. This bill is not about cyber security but about intelligence.]**

# DEPARTMENT OF DEFENSE APPROPRIATIONS ACT 2015

## Funding for NSA to add back doors to equipment cut

<http://www.cnet.com/au/news/house-oks-measure-defunding-nsa-backdoor-surveillance/>



# CHINA CYBERSECURITY LAW

**Allows China Government surveillance of commercial activities, tech companies.**

- **Legalises what they do anyway.**
- **Opposed by US, AU businesses.**

<https://www.itnews.com.au/news/china-to-implement-controversial-cyber-security-law-463468>

# SOMETHING TO THINK ABOUT

## **Are:**

Employers now permitted to read employees' e-mail / web without consent?

Is this only spying agencies / police ?

• • • • • • • •  
• • • • • • • •  
• • • • • • • •

# Illegal Activities

• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •  
• • • • • • • • •

# Fraud

# Fraud

## **Investment fraud**

The criminal buys worthless stock, artificially inflates the value (by seeding rumours of some new development), sells it at a profit

## **The Nigerian scam**

A [deceased] government official e-mails you and asks for your assistance in transferring money out of his country, for which you will receive a commission. You send money to pay for taxes and expenses

## **Auction fraud**

You buy an item from an auction site, send the money and the item never arrives

## **Romance Scams**

# Fraud prevention

**Only use legitimate investment brokers**

**Don't respond to un-solicited e-mail**

**Use well-known auction sites only**

Read the seller's feedback

- The feedback for sales, not purchases

# Money Laundering

Hi Mate [jhamlynharris@swin.edu.au](mailto:jhamlynharris@swin.edu.au),

Are you a college student with odd class schedules impairing regular work time? Are you jobless sitting at home and connected to the Internet? We are looking for honest and communicative people to sort, store, and make readily available our delivered correspondence from your own home.

There is no necessity to visit any office for this job. You can do your job sitting at home. You need only to check your email twice a day to be informed about job processing. This will take a few minutes of your day. This is not a sales gimmick requiring you to pay set-up fees or sign up to a mailing list. This is a business requiring only limited amounts of your time. You will earn money even without going out of your house or office. The job is regular the wages are solid. Spaces are limited so act now for this great intuitive job offer.

Job short description:

This job consists of 3 steps.

1. You receive packages from shops (stores). Before receiving the packages you are informed about it by e-mail or phone. The packages are delivered by courier such as UPS, FedEx, DHL, Startrack, Courierplease and TNT.

2. When you receive all orders (package by package), you collect them in one whole box. Then receive money to post it or it may be picked up by courier service. You don't have to pay anything.

3. After the package is sent, you receive an e-mail during 48 hours where is a Money Transfer Control Number of Western Union. Now you suppose to visit the nearest bank and get your salary. For every sent package your salary is \$100. So if you are hard working you can earn more in a week.

Already ready to deal with us? Drop your full name, your age and current address to:

Email: [Josh@deliveryman.com](mailto:Josh@deliveryman.com)

Josh Carrington  
Mobile: 0457355509  
Tel: 0280074797

# Ethics



## Ethical dilemmas for network admins:

Is it OK to read your users' mail?

Use remote desktop?

let your users print their kids' assignments?

let your users take paper home?

let your users send private e-mails?

let your boss use company resources for his private consulting business?

let your boss download mp3s?

# Ethics

## Ethical dilemmas for network admins:

### Legal / Illegal

Is it OK to read your users' mail?

Use remote desktop?

let your users print their kids' assignments?

let your users take paper home?

let your users send private e-mails?

let your boss use company resources for his private consulting business?

let your boss download mp3s?

# Ethics

## Who maintains the web sites / databases of shady web sites?

- gambling
- adware
- cracker sites
- Moderating sites (game consoles)
- pornography
- paedophile forums

## What will you do if offered a job maintaining such as site?

# Ethics

- What are your responsibilities to your profession?
- Public Interest takes precedence over the other values
- Not knowingly mislead a client
- Give credit for work done by others where credit is due
- Give realistic estimates for projects

## ACM Code of Ethics

<https://www.acs.org.au/search.html?q=Code+of+ethics>

# Ethical Dilemmas?

**Sys admin for Black Market Reloaded?**

**Protect and promote the health and safety of those affected by your work**

# Identity theft

# Identity theft

## **The criminal collects enough information about the victim to**

- conduct on-line transaction in the target's name.
- convince banks / governments to issue credit cards, driver's licences, and potentially passports.
- In Australia, you need 100 points of documentation to prove your identity

<http://www.eaussie.com.au/images/pdf/Aussie100PointForm.pdf>

Looks like a shopping list for a dumpster dive.

## **Information may be collected by**

- using Google.
- using government and genealogy web sites.
- dumpster diving at your work / home.
- asking your co-workers casual questions about you.
- packet sniffing.

# Identity theft protection

- **Reveal as little as possible to web sites**
- **Construct an alternate identity (separate e-mail address, modified version of your name)**
- **Shred all documents before disposal**
- **Do data mining on-line to see what attackers can see about you (ego-surfing, checking VicRoads, government and CityLink web sites)**
- **Lock down your browser (disable scripting, password storage, cookies)**



# Paranoid?

- **Boot from a read-only Linux distro**
- **Use a diskless workstation**
- **Disable JavaScript**
- **Sandbox all applications**
- **Tunnel all network traffic through TOR / VPN / Tor hidden services / ProXPN**

# Really Paranoid?

## Use a burn PC

- Tails OS
- Use once, throw away
- Use somebody else's PC
  - preferably in China

# Stalking

# Stalking

- Threatening e-mails.
  - Pornographic e-mails.
  - Spoofed\* (and defamatory) Facebook pages
  - Spoofed e-mails.
- 
- Create a false identity with nothing in it to connect it to you.
  - Keep all threatening e-mails, etc.
  - Report to WHO@ <http://www.haltabuse.org>

# Spam and "Helpers"

- Companies who use spam ("push advertising") and browser hijackers (targeted marketing tools) insist that they operate legally (and ethically)
- These companies operate in the grey area of the law, often through a chain of other parties
- Google participates in some of these chains
  - <http://www.google.com.au/intl/en/ads/>
  - Is this a scam? <http://getgoogleadsfree.com/>
- How about this? <http://www.perrymarshall.com/google/>

# Filtering

# Porn Filtering techniques

## Parental Control Tags:

- Must be implemented by the web site. Not all are ethical

## Clean feed:

- Filtering of Australian internet proposed (2008) and then abandoned by previous government

<https://www.efa.org.au/2011/01/12/europe-gets-it-filters-dont-protect-children/>

<https://www.efa.org.au/2012/11/09/internet-filtering-backdown/>

## Image filtering:

- Still in it's infancy
- Proposed in 2008

<http://www.somebodythinkofthechildren.com/sunday-wrap-up-image-filter-mistakes-conroy-for-porn/>

- One classifies George W Bush as offensive material

<http://www.dansdata.com/pornsweeper.htm>

# Porn Filtering techniques

**Pornography filtering uses blacklists, keywords and parental control tags**

## **Blacklists:**

- Filter by IP address, domain name
- Reactive security measure which will not filter new web sites
- Whitelists are better.

## **Keywords:**

- Cause false positives and false negatives

<http://www.news.com.au/porn-filter-fails-say-web-experts/story-e6frfkp9-1111115235591>

<http://www.techdirt.com/articles/20090803/0323345754.shtml>

- "intelligent keyword" filtering uses a keyword score?



# Porn Filtering Tools

- If running as administrator, can be uninstalled/disabled by anyone.
- **Ordinary users may be able to kill the process with Task Manager**

- Some use Root-kit technology to prevent user from killing process

<http://www.netdogsoft.com/>

“No Process will be found when running, NetDog Porn Filter works quietly in the background when surfing on the internet ! ”

# Porn Filtering Tools

**Most kids are more computer literate than their parents.  
This one disabled NetAlert in 30 mins**

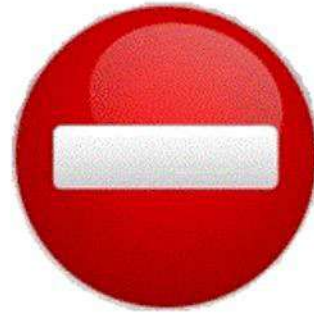
- To prevent tampering on the PC, install the filter at the ISP

[http://www.zeropaid.com/news/9749/australian\\_government\\_to\\_finance\\_faulty\\_internet\\_filtering\\_technology/](http://www.zeropaid.com/news/9749/australian_government_to_finance_faulty_internet_filtering_technology/)

**Filters don't work:**

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2002/11/13/BU158763.DTL>

# Blocking



## Access Blocked

Access to this site has been blocked by an order of the Federal Court of Australia because it infringes or facilitates the infringement of Copyright.

If you think you have been redirected to this page incorrectly, please contact your service provider.

# Piracy site blocking – 57 more

- **Started in 2014**
- **Not successful**
- **Resumed/renewed push August 2017**
  - <http://www.abc.net.au/news/2017-08-18/pirate-sites-to-be-blocked/8820076>
  - <https://torrentfreak.com/court-orders-aussie-isps-to-block-dozens-of-pirate-sites-170818/>

# Technology: fake certificates + HTTPS

## “We Got Past The Government's Anti-Piracy Blocks In Five Seconds”

<https://www.kotaku.com.au/2017/02/we-got-past-the-governments-anti-piracy-blocks-in-five-seconds/>

## ISPs were left to choose their own methods of site blocking


- URL block or a DNS-based redirection

# VPN

Bookmark Ctrl + D

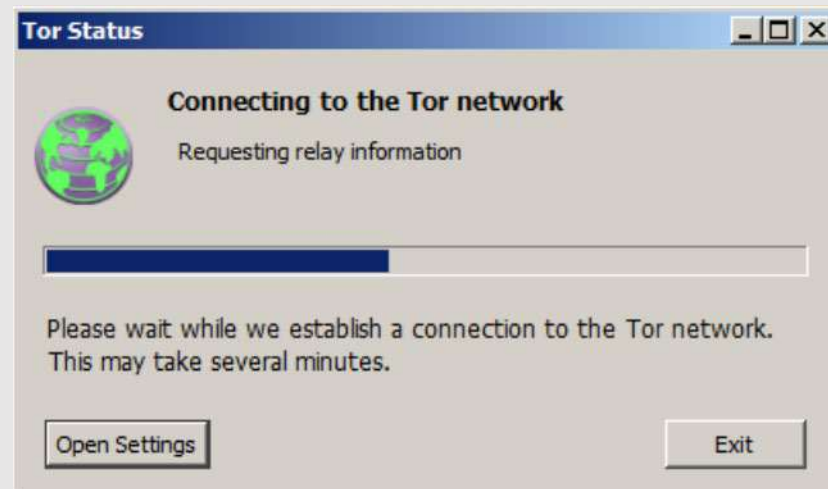
Proxy unblock not working? [Click here](#) for a VPN and **unblock all torrent sites**

Torrent Proxy	Speed	Status
<a href="https://eztv.unblocked.bid">https://eztv.unblocked.bid</a>	very fast	ONLINE
<a href="http://eztvproxy.com">http://eztvproxy.com</a>	fast	ONLINE
<a href="http://eztv.rocks">http://eztv.rocks</a>	fast	ONLINE
<a href="https://eztv4-ag.unblocked.lol">https://eztv4-ag.unblocked.lol</a>	fast	ONLINE
<a href="http://eztvmirror.com">http://eztvmirror.com</a>	fast	ONLINE
<a href="https://eztv-ag.unblockall.xyz">https://eztv-ag.unblockall.xyz</a>	fast	ONLINE
<a href="https://eztv.unblocked.bet">https://eztv.unblocked.bet</a>	very fast	ONLINE
<a href="https://eztv.bypassed.cool">https://eztv.bypassed.cool</a>	very fast	ONLINE

 show all proxies 15

Torrent proxy sites and mirrors let you bypass firewall and ISP restriction and access blocked torrent sites like EZTV.

# Tor Browser





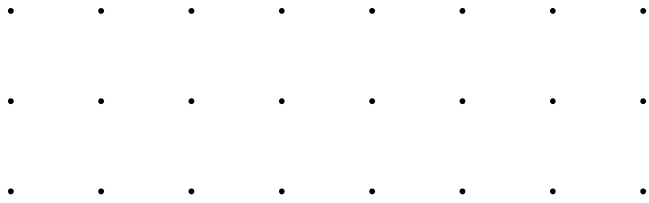


# Stuff you can't do (legally)

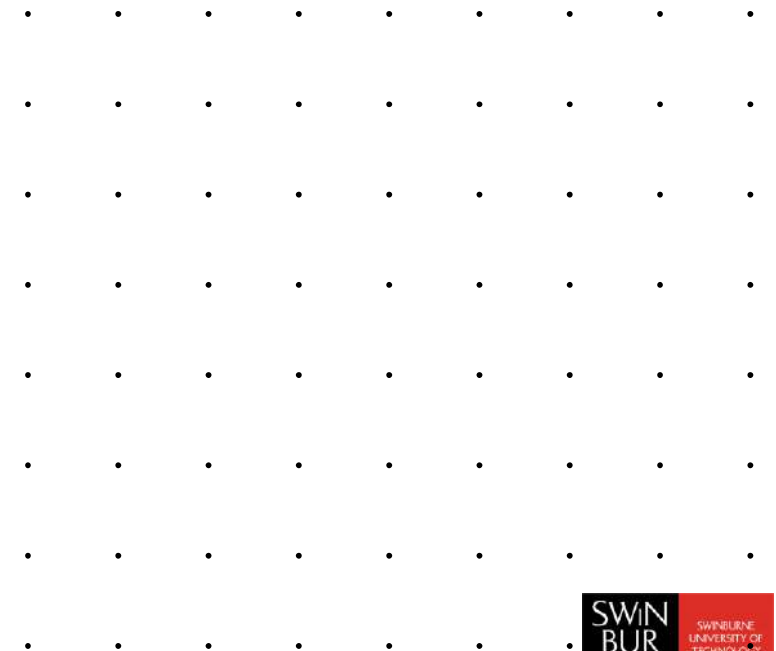
- **Perform a DOS on a spammer**
- **Release a virus that disables bots or zombies**
- **Release a worm that patches software or removes security vulnerabilities**
- **Contact the owner of a zombie and tell them they're 'owned'**
- **Pen-Test your own network**
  - But you can if it's off the internet

# Stuff you can do

- **Block packets from a zombie's IP address**
- **Offer to disinfect your auntie's computer**
- **Contact the ISP of a suspected spammer**
- **Report new worms and Trojans**
- **Report new scams and hijackers**
- **Use white-lists**
- **Become a system administrator and create non-root accounts for normal use (even your own)**



# eForensics



## **Discovery and analysis of evidence of Computer Crimes**

- Crimes against computers
- Involving computers
- Or, where computers contain evidence of non-computer-rated crimes

# Types of eForensics

## Network forensics

- Packet capture, logs – record evidence while the crime is occurring.
- Cloud forensics – relies on cooperation of cloud provider, cloud API, foreign government.

## Disk forensics/phone forensics

- Live (no re-boot)
- Dead/offline/static (boot into another OS)
- Acquisition (of drive image)
- Acquisition (of RAM)

# Types of Forensics

## Memory forensics

- Contents of RAM,
- running processes,
- active network connections (TCP) and
- Traffic (UDP)

# Disk Forensics

- **Different sorts of evidence available depending on platform, OS, file system.**
- **Want to get meta-data as well as files.**
- **Meta-data provides nexus information:**
  - Who, what, when, where.
  - Proof that the suspect did the crime.
  - Who's account did they use?

# First steps

- **Secure crime scene, confiscate computer.**
- **Record all running processes,**
- **Record system time (compared to actual time)**
- **Record partition details, drive mapping**
- **If drive cannot be imaged, plug in a write-blocker**
  - Prevents metadata from being changed



# Use toolkits

## **Linux Distros.**

- Caine
- Backtrack
- Knoppix
- Helix
- SANS SIFT

**FTK (Forensic ToolKit)**

**TSK (The Sleuth Kit)**

**Autopsy (front end for TSK)**

**EnCase (Windows)**

# Steps

- 1. Make a forensic copy of drive.**
- 2. Calculate a hash of the copy for later.**
- 3. Record the time on the computer, compare with actual.**
- 4. Impound drive as evidence.**
- 5. Note down everything that follows so that another forensic expert can find the same evidence.**

# Analysis of Image

1. Load into tool, check hash.
2. Search for deleted files.
3. Search for re-named files (esp. file extensions).
4. Search for encrypted containers.
  - Use entropy analysis to determine type of encryption.
  - Search drive for password reminders...
5. Search for keywords in files.
6. Search for e-mails, shortcuts, file shares, favourites, cached web files.

# File Carving

1. **Search for keywords in deleted file space (even if it's reformatted, repartitioned).**
2. **Find sectors containing keywords**
3. **Find iNodes containing sectors**
  - Or find starting signature, end signature sectors.
4. **Copy sector range to file**
5. **View**

# Found evidence?

1. When files “of interest” are found, record metadata, copy of file, file location.
2. Dates are very important – establish a time-line which reflects the sequence of events during the crime.
3. If Wireshark captures or logs are found, use these to confirm times, sequence of events.
4. Check hash again.
5. Write report.