UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 2 part 2

24 September 2019

Topics for this lecture

1. A diversion for Time

2. Windows forensics #2
    1. Useful artefacts
    2. Antiforensics

A short diversion for TIME

- When TIME is used to contextualise events, interpreting the correct (or real) time is essential
- Consider the following interactions which are exactly the same words – de-identified but taken from a real case

Hey, are you awake yet?

Did you rob the shop last night?

Yes

Tell me more about what you did last night?

No

Mum reads my messages so I'll call you later

The prosecution's initial evidence

Hey, are you awake yet?

Yes

Did you rob the shop last night?

No

Tell me more about what you did last night?

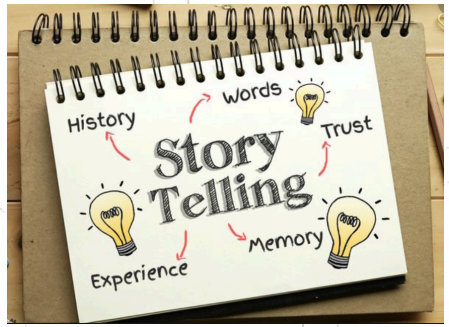
Mum reads my messages so I'll call you later

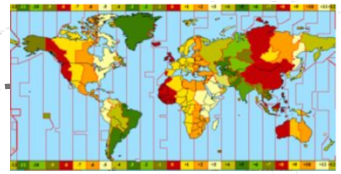
When sequenced correctly
-- prosecution withdrew their earlier version

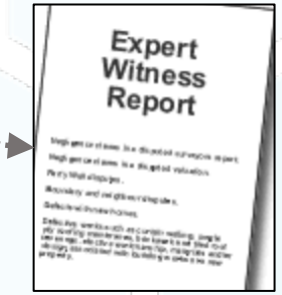
Interpreting time

Time is the anchor data for sequencing events, however it is also the data that causes so much confusion.

Time for a war story…







Time synch and common problems

- For Australia, the official time source is (or rather should be) the synchronisation service provided by the National Measurement Institute[1]. NTP servers in:
  - Adelaide
  - Brisbane
  - Melbourne
  - Perth
  - Sydney

- Interestingly, most commonly used time sources use others e.g. Google[2], Pool[3]

It is not a new problem
Iconic WW2 image of synchronising watches

1. §8AA of the National Measurement Act requires the Chief Metrologist is to maintain this
2. See https://developers.google.com/time/
3. See https://www.pool.ntp.org/zone/au

Time synch and common problems (cont)

- Some commonly encountered problems
  - Adjusting across days
  - dd-mm-yyyy and mm-dd-yyyy
    - for the first twelve days
  - Daylight savings
  - Windows versus Unix/Mac time
  - 1900 and 1904 serials
  - First person adjusting and then next person adjusting, etc
  - Same source provides in different formats
  - For long events, is it the start time or the finish time?
    - What does the Electronic Transactions Act has something to say about this for commercial transactions?

Asking for one months data solves both of these

Timezones and representations of time

- National Measurement Act requires UTC

- Coordinated Universal Time (or UTC) was originally specified by *Bureau International des Poids et Mesures* (BIPM) in 1967.

- **ISO 8601** – Data elements and interchange formats -- Information interchange -- Representation of dates and times (currently being revised)

- **IETF RFC 3339**[1] - Date and Time on the Internet: Timestamps (2002)
  - Offset [±HH:MM] refers to local time
    - Is the computer's clock adjusted for daylight savings?

ACTIVITY

- Spend 5 minutes writing 2-3 paragraphs describing UTC, GMT and Zulu times
- Discuss it with your neighbour
- Anyone want to share?

Date should be shown as yyyy-mm-dd. In practice not all service providers use this, instead adopting their national one e.g. Apple uses mm-dd-yyyy

1. RFC 3339 is part of the optional readings for this week
2. An history of UTC is given by BIPM and is included in the reading. Also see https://www.bipm.org/cc/CCTF/Allowed/18/CCTF_09-32_noteUTC.pdf

Sample answer

Coordinated Universal Time (shortened to UTC as a compromise to the French speakers) is a standard adopted in 1967 for calculating date and time based on the International Atomic Clock and is maintained by the *Bureau International des Poids et Mesures* (BIPM) in France. It includes ways of representing date and time which have since also been standardised as ISO 8016. UTC is not adjusted for daylight savings.

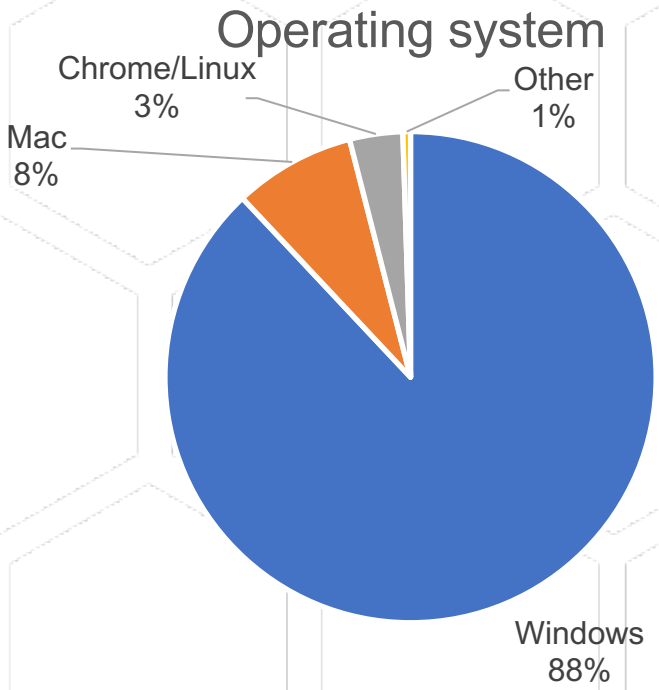
Greenwich Mean Time (or GMT) is a time zone that is at the Greenwich meridian, which is also the zero meridian. **Zulu** (or Z) refers to the timezone at the zero meridian and for practical purposes is equivalent to GMT. Local times are shown are ±Z. For example, a timestamp affixed in Sydney will show as +10:00 meaning 10 hours ahead of Zulu/GMT (or +11:00 in daylight savings).

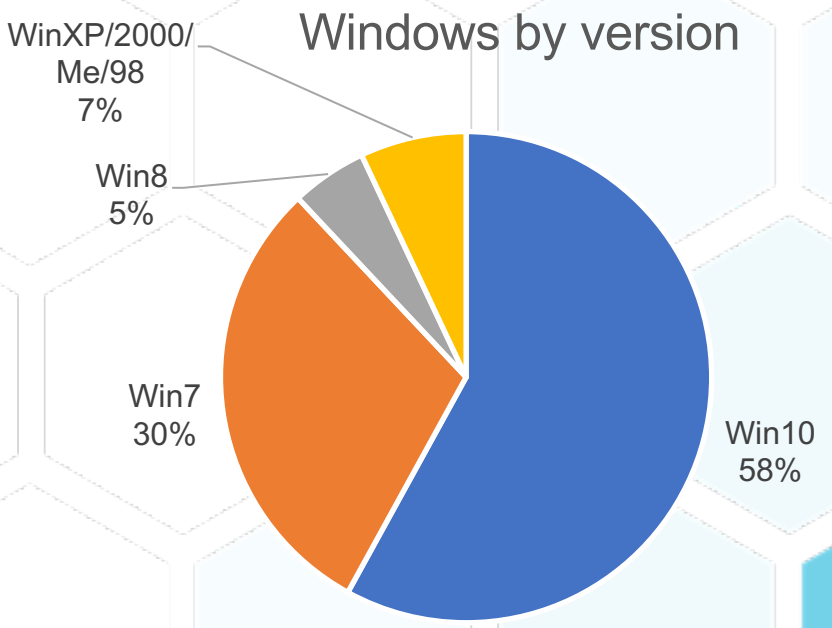
The difference between UTC and GMT varies according to the year and in 2019, the difference is less than 1 second. Many timestamps use UTC, GMT and Z interchangeably. For the purposes of my report I will use GMT (*pick one and stick to it*).

Windows forensics #2

Operating systems on desktop/laptop

Popularity of Windows means it is the most commonly submitted for examination





Based on data from Computerworld's Windows by the numbers

What things do we need to examine?

- Really depends on the circumstance of the case
  - A document showing something
    - Remember a document is also picture, video, audio, etc
    - Metadata is merely a document showing something about another document
  - Communications between people
  - Recording of something sensed by the computer or of calculations made by the computer
    - Often called a log file
  - Communications between computers

What things do we need to examine?

- What things would you want to prove for:
  - Human generated document
    - A recording of human input e.g. typing, voice, etc
      - An accurate representation of the human generated content
  - Computer generated
    - Without the intervention of a human
      - Outcome of a process
      - Process was reliable, predictable and repeatable (given the same inputs, you get the same output)
  - A combination of the above

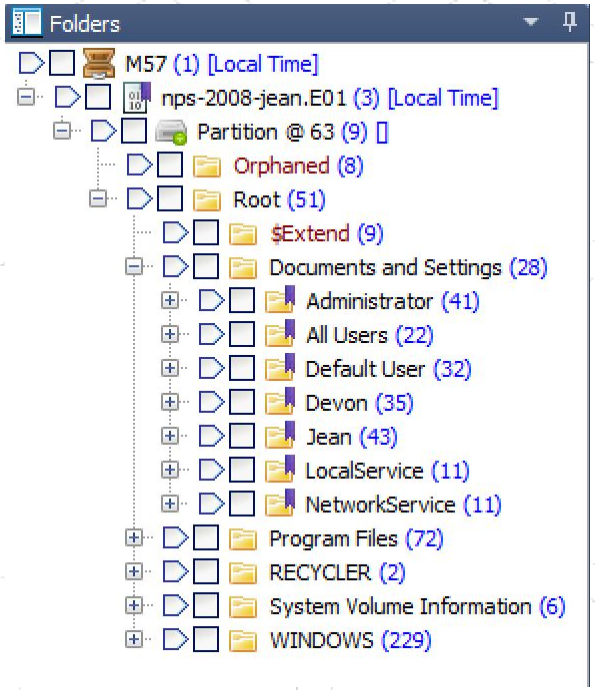
There is a specialist field on software reliability which is defined by ANSI as: *the probability of failure-free software operation for a specified period of time in a specified environment*

⇩

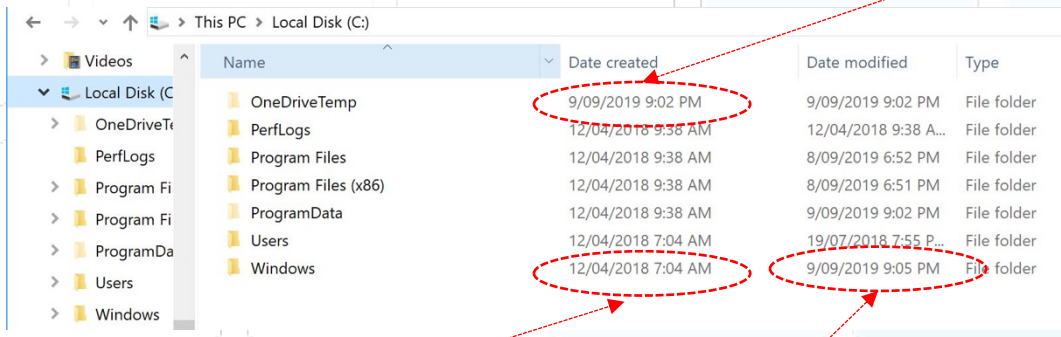
Remember what I and the Magistrates said about stepping outside of your expertise

A typical Windows computer

- WinXP viewed using Forensic Explorer



- Win10 viewed using File Explorer
- What does it tell us?

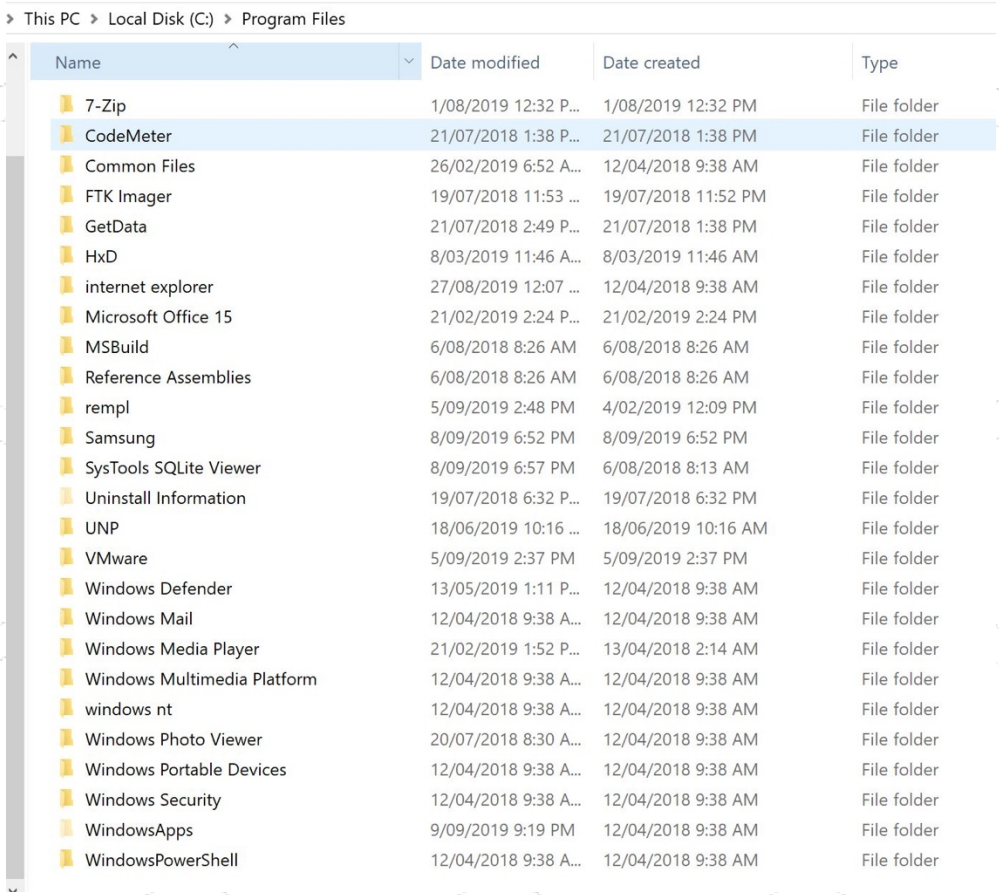


User had Microsoft account sync with OneDrive

When Win was installed

When Win was being used

Simple things can be a give-away



- The Program Files directory shows when programs were installed i.e. Creation Date

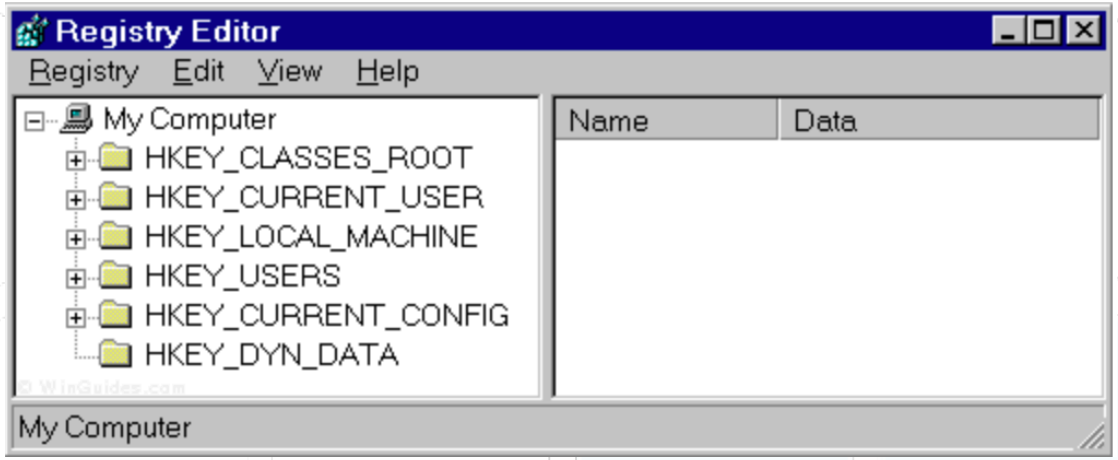
- ANZ v Kelly[1] has become the precedent (i.e. textbook) case for proving a PDF file was forged
  - The fact that certain software was not yet published at the date it was apparently installed indicated tampering of the computer's clock

1. http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2014/426.html

The Registry

- Is a fancy name for a set of configuration files

- **HKEY_CLASSES_ROOT** - file association mappings, OLE information, Windows shortcuts, and core aspects of the Windows user interface.
- **HKEY_CURRENT_USER** - for the user currently logged on e.g. logon names, desktop settings, Start menu settings, etc
- **HKEY_LOCAL_MACHINE** - computer specific information about the hardware, software, and other preferences. Used for all users who log onto this computer.
- **HKEY_USERS** - Individual preferences for each user of the computer, each user is represented by a SID sub-key.
- **HKEY_CURRENT_CONFIG** - This branch links to the section of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.
- **HKEY_DYN_DATA** - for use with the Plug-&-Play features of Windows, this section is dynamic and will change as devices are added and removed from the system.



Pre-Win7

- Windows 95 & 98 in two hidden files in your Windows directory, called USER.DAT and SYSTEM.DAT
- Windows Me there is also a CLASSES.DAT
- Windows NT/2000 the files are contained separately in the %SystemRoot%\System32\Config directory

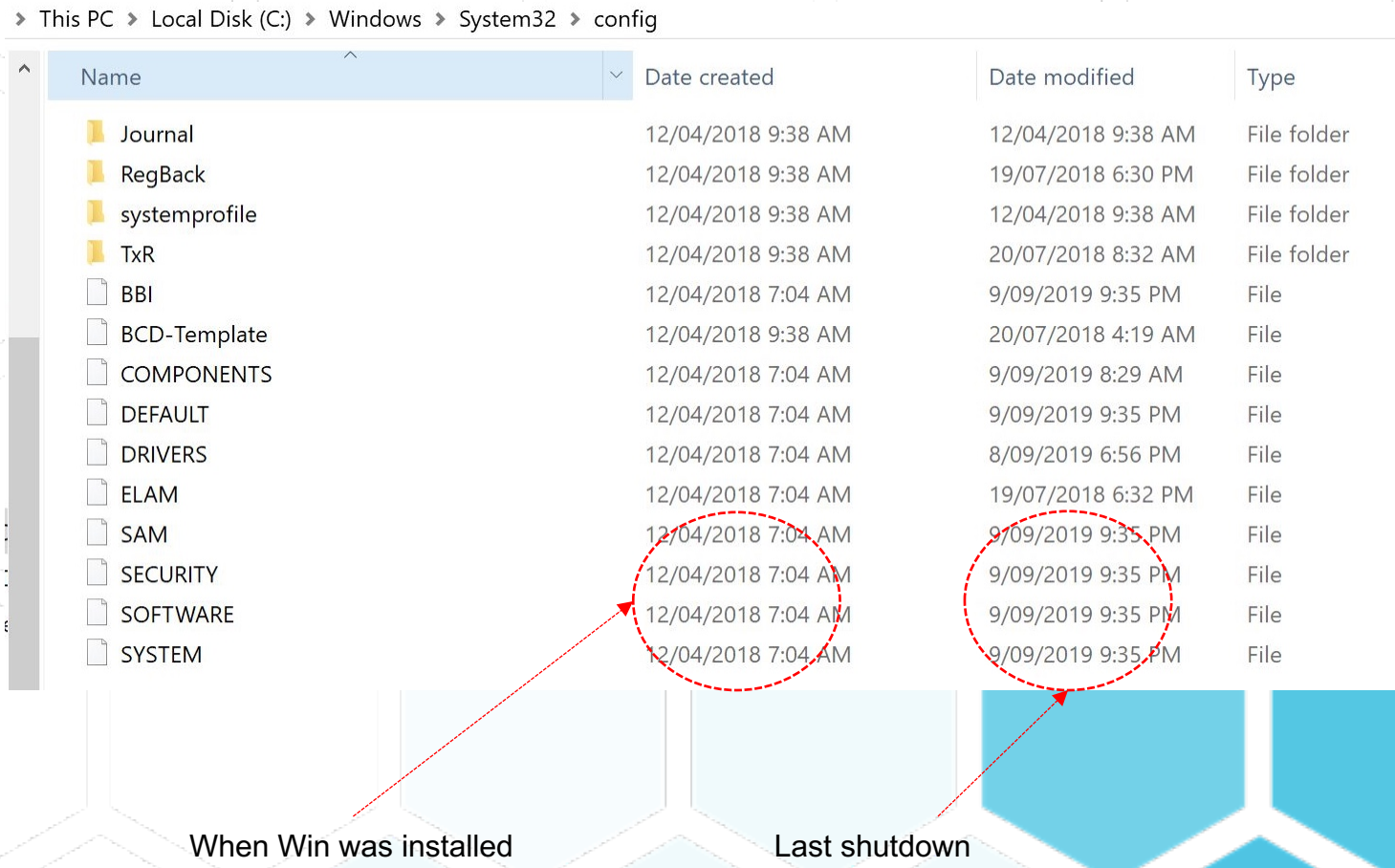
Registry Win7+

REGISTRY FILES

- HKEY_LOCAL_MACHINE \SYSTEM : \system32\config\system
- HKEY_LOCAL_MACHINE \SAM : \system32\config\sam
- HKEY_LOCAL_MACHINE \SECURITY : \system32\config\security
- HKEY_LOCAL_MACHINE \SOFTWARE : \system32\config\software
- HKEY_USERS \UserProfile : \winnt\profiles\username
- HKEY_USERS.DEFAULT : \system32\config\default

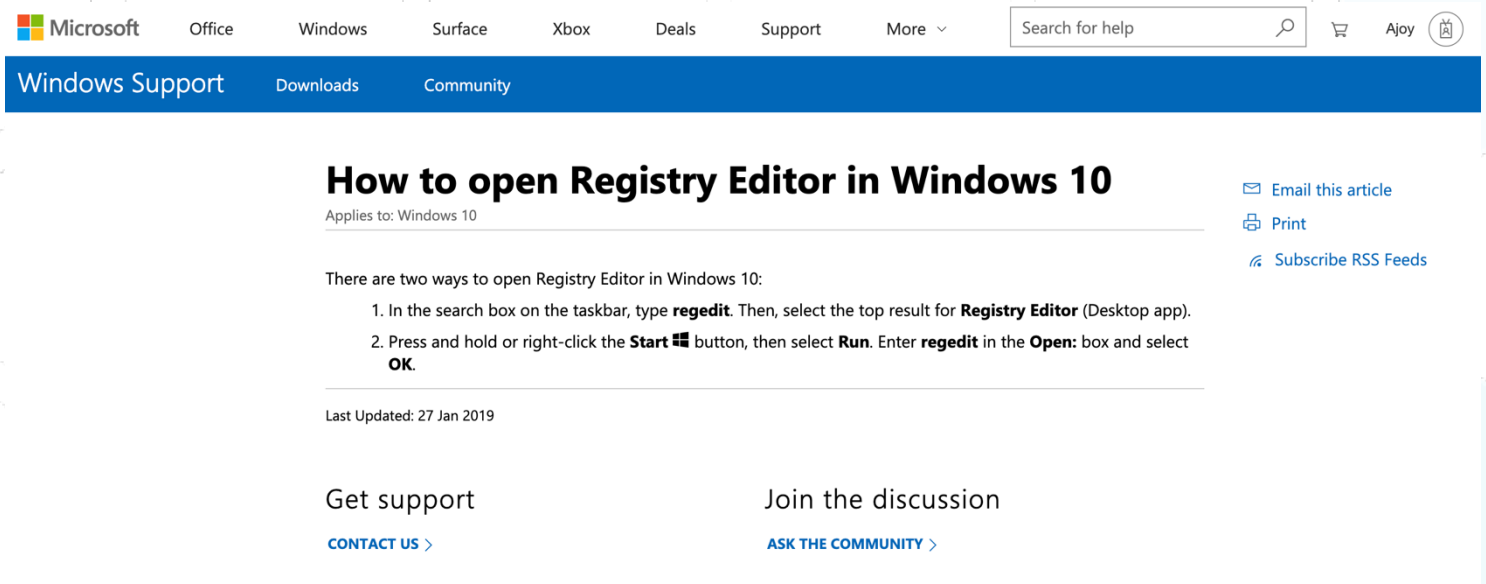
VOLATILE REGISRTY (IN MEMORY)

- HKEY_LOCAL_MACHINE \HARDWARE : Volatile hive
- HKEY_LOCAL_MACHINE \SYSTEM \Clone : Volatile hive



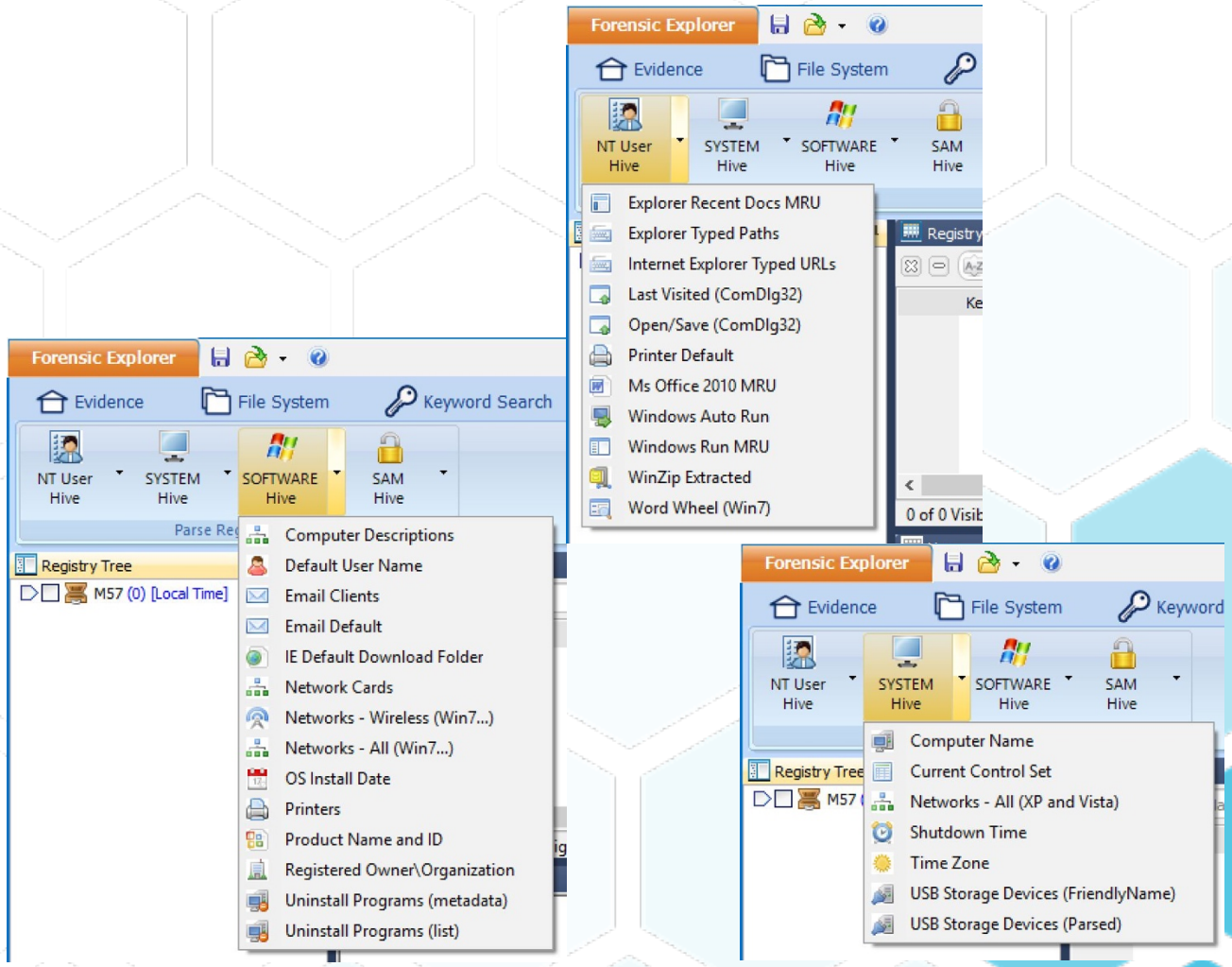
Referencing the source

- It is important to reference the source, when you can reasonably be expected to have done so
- It is reasonable to reference Microsoft as the manufacturer of the Windows software
  - Use their official documentation



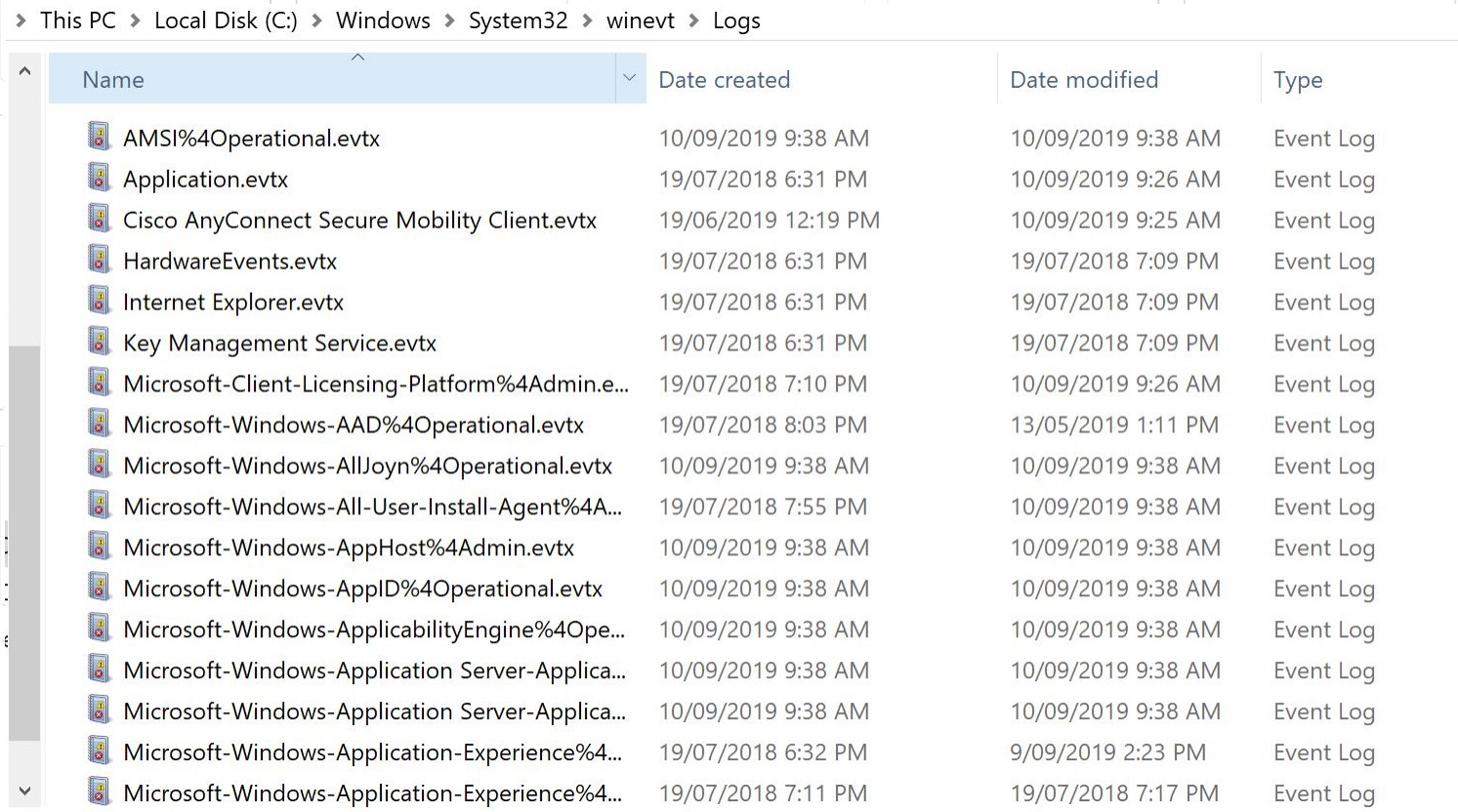
Good forensic tools have tools to parse the registry

- These are from Forensic Explorer and using the M57 case study
  - on WebCMS



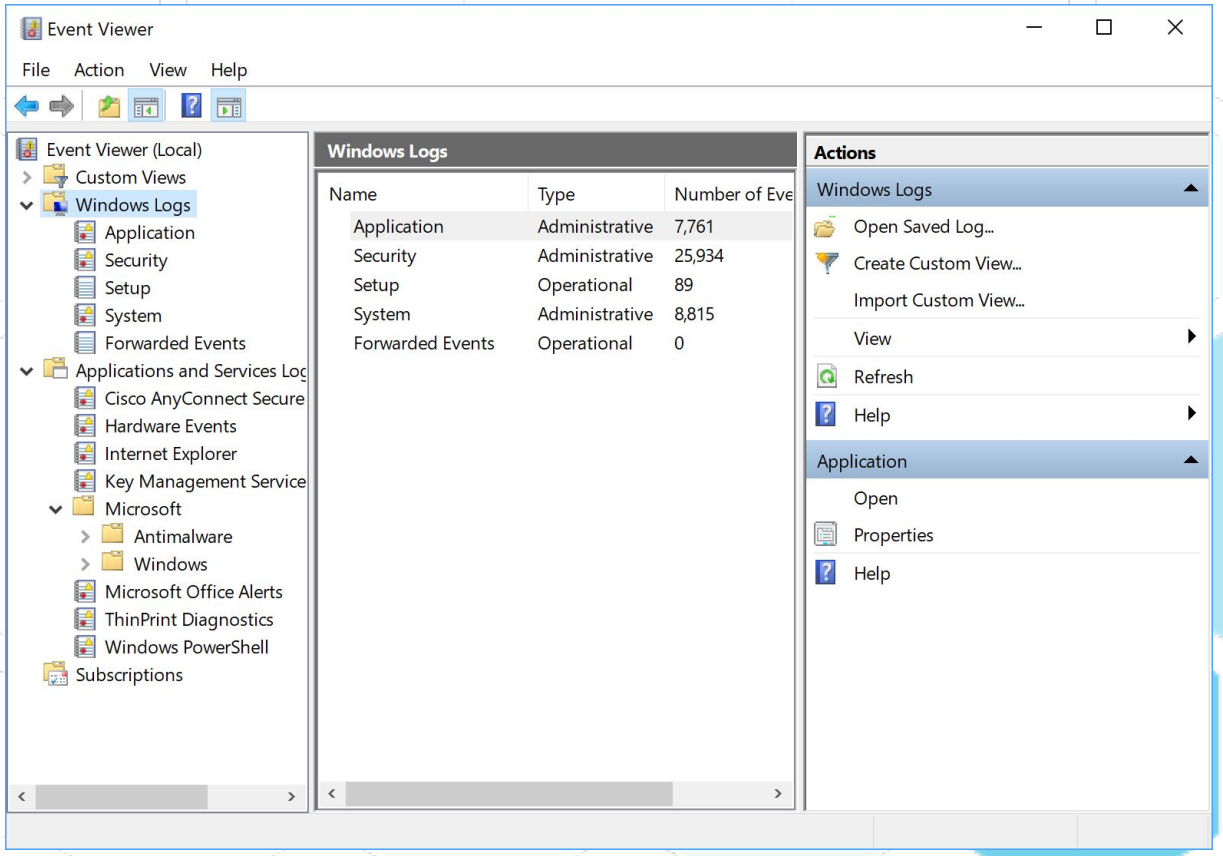
Log files

- Windows\System32\winevt\Logs
- Need to be interpreted



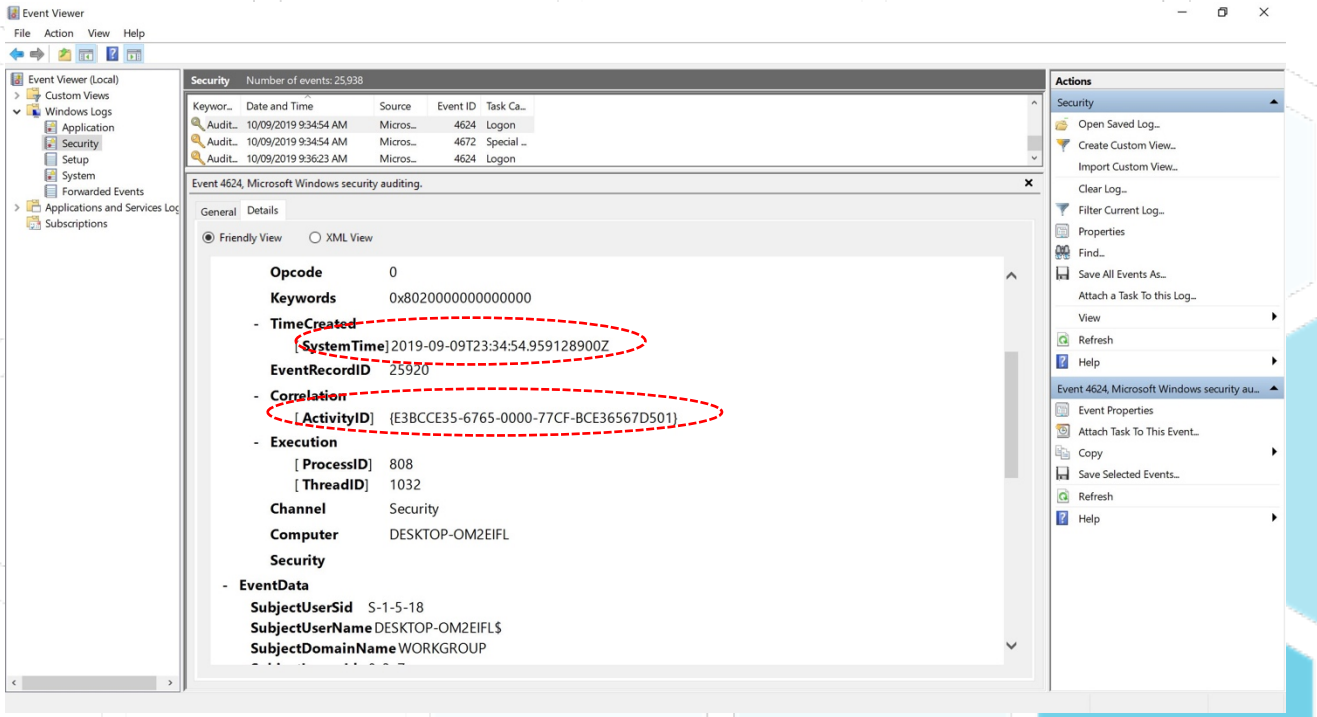
Windows Event Viewer

- Shows different logs. Key ones are:
  - Application
  - Security
  - System
  - Application and service logs



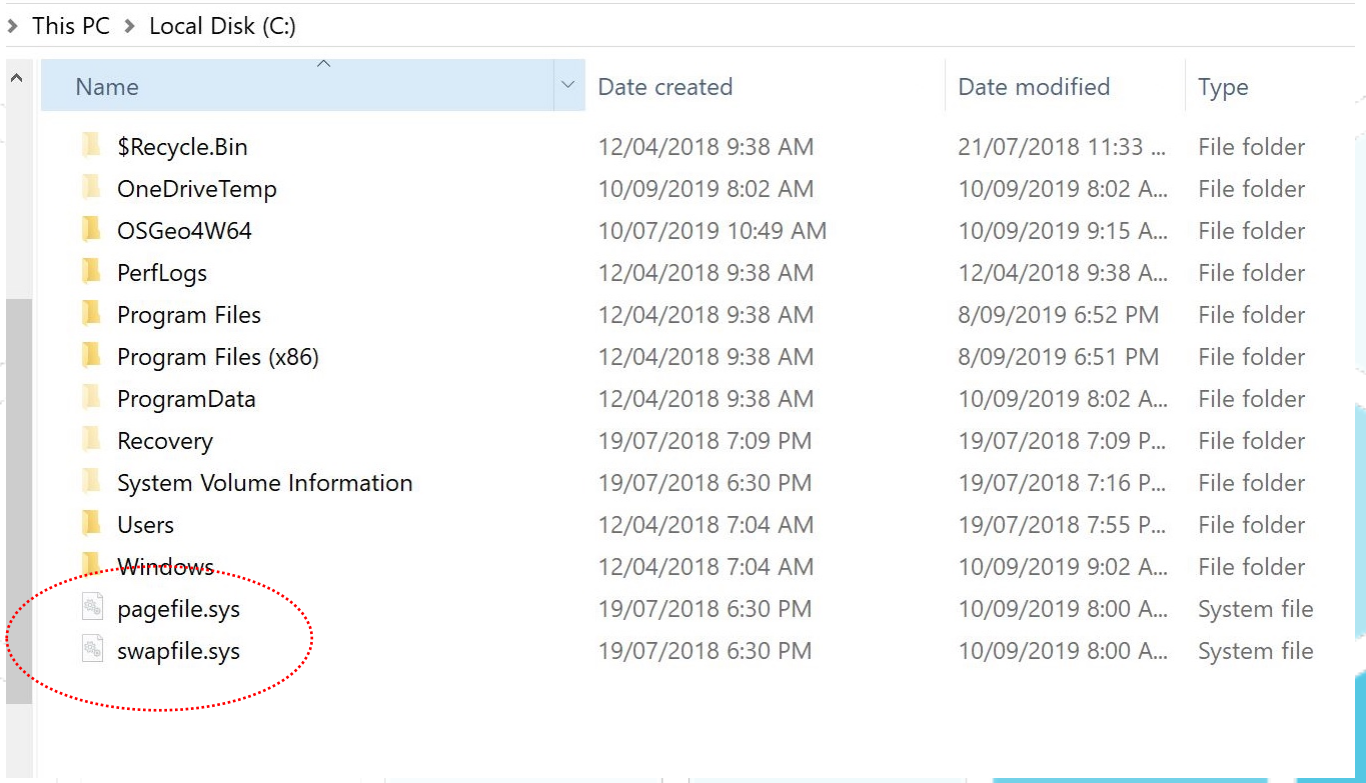
Detail is important!

- Should take *prima facie* i.e. on face value. Small changes in detail indicate further enquiry
  - A missing event indicates something odd is happening
  - A mismatch between sequence (EventRecordID) and Time indicates change to system clock



Virtual memory

- System files in root directory
- For Win10, hibernation is not always supported so hiberfil.sys may or may not be there
- WE WILL EXPLORE THESE MORE NEXT WEEK



Antiforensics

Every click you take, they'll be watching you

The law has a new high-tech stool pigeon reporting criminal activities, writes **Amber Hunt**.

Got an iPhone in your bag? Chances are you may be storing even more personal information than you realise, and some of it could be used against you if you're ever charged with a crime.

A burgeoning field of forensic study deals with iPhones specifically because of their popularity, the demographics of those who own them and what the phone's technology records during its use.

Two years ago, as iPhone sales boomed, a former hacker, Jonathan Zdziarski, decided law-enforcement agencies might need help retrieving data from the devices.

So he set out that turned int *Forensics*. That being tapped by nationwide to t information is s

50 million iPhones, according to company figures. Clearing out user histories isn't enough to clean the device of that data, said John Minor, a communications expert and

mapping functions, as well as various global positioning system applications.

The free application Urbanspoon is primarily designed to help users locate

Thieves ensure raising goes off with bang

Brad Howarth
Database

AUSTRALIAN

THE IMPOSTORS

THE REAL NICOLE McCABE

JOSHUA BRUCE'S MOTHER

I am fearful, but hopefully everyone will see that it is fraud.

THE VICTIM

Messy job: Police investigate the break-in and safe cracking at GroovyChannel's offices

Facebook failed to tell police about paedophile porn ring

Dylan Welch

FACEBOOK management failed repeatedly to reveal the activity of an international child pornography syndicate operating on their site and ignored continuing admissions by one of the ring's Australian members.

The failure by the social networking site was uncovered during a federal police-led international investigation of the syndicate, which had been using fake online identities.

"We are aware that Facebook knew of the existence of these pages and even went so far as to remove the profiles," said the director of the AFP High Tech Crime Centre, Neil Gaughan.

But despite closing down the pages after finding illegal material, Facebook did not contact police, Mr Gaughan said.

"Facebook deactivated the online accounts of the initial suspects but there were indications that, within hours, the groups were re-forming again."

The taskforce, codenamed Project Ocean, was set up by the AFP in March. By June it included the FBI in the US, the Child Exploitation Online Protection Centre in Britain, the Mounted Po Germany, Switzerland.

While off may have be involved in men have b include two aged 33 and

old from Port Kembla. The British-based man police say is the ringleader was due to face an English court overnight.

All 11 are accused of creating

company failed to pass the information to police.

Federal police also contacted a Facebook official in Australia to convey their concerns, and

tacted for comment yesterday. However, a Sydney public relations company that works for the company sent the *Herald* quotes made by the company's chief

"Graphic images"... one of the accused men. Photo: Robert Peel

TRACKING YOUR EVERY MOVE

- Every time an iPhone user closes the built-in mapping application, the phone snaps a screenshot and stores it.
- iPhone photos are embedded with tags and identifying information, so photos posted online might include GPS co-ordinates of where the picture was taken and the serial number of the phone that took it.
- Even more information is stored by the applications themselves, including the user's browser history, which could prove useful to police.

tories and text messages most useful in homicide cases. But Zdziarski, who has helped federal and state law-enforcement agencies

Apple doesn't store that cache very securely, Zdziarski contended, so someone with expertise could recover months of typ-

- Four common categories

1. Avoid recording
   - Recording the wrong things;
   - Using services knowing recordings aren't made or are going to be hard to get;
2. Hide recordings;
3. Expunging or destroying the recording;
4. Changing the recording.

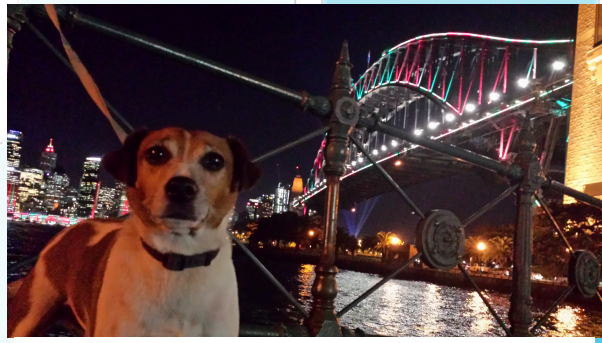
Can you think of examples?

Avoid recordings

- Use of public computers and public wireless
  - e.g. Sydney collar bomb extortionist
- Steep increase in use of secure email
  - e.g. Protonmail, Hushmail, Tutanota
- Change identifiers
  - Use of VPNs, change MAC, etc
  - Being built-in to consumer products in the name of privacy
    - e.g. Apple now scramble browser signatures
- Use of these services might indicate something to hide. Might also indicate the person values their privacy.
  - A give-away might be when they start using a service or selectively use a service

Hide recordings

- Use codes and encryption
  - Low tech is favoured by drug dealers, jihadists, etc
- Use encryption to hide in plain sight
  - e.g. Steganography, multiple containers, etc
- Hide in plain sight
  - e.g. draft of email but don't send
- Physically hide
  - e.g. use of detection dogs



Benji is my USB/mobile phone detection dog (now retired)

Many tools to expunge or change data

- CC Cleaner, Disk Doctor and Norton Clean are most commonly encountered in our practice

- Some work better than others…but there is always stuff left behind
  - File fragments
  - Pre-fetch files
  - Virtual memory
  - Application data, backup data and data stored in cloud

Need to find correlating data

```
Received: (qmail 27394 invoked by uid 30297); 15 Jul 2019 19:00:53 -0000
Received: from unknown (HELO p3plibsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
          (envelope-sender <fecdev@yahoo.com>)
          by p3plsmtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
          for <info@proksimiti.com>; 15 Jul 2019 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
  (Client did not present a certificate)
  by CMGW with ESMTP
  id n6DUhF6dMOiyon6DUhGLMC; Mon, 15 Jul 2019 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240;
bh=8X7yayAIb3rM/ntRAK51gp9Em0JURK/p+ksVu/Z551U=; h=Date:From:To:Subject:References:From:Subject;
b=tQ1O9lbhlhas/87XFPpUNlysUhIYzDVm42L4MC6i6iofZ2+jslT5u5yAQB9fwxniIaEY4fQ6aTGK1BJn3WI967WUwAN0d4uYide8NwM1uSzD4p68muVqv85PrkbwEDIx
L7deohpTgiI93T84I5skBGiWw4BisqkG9b52RaBa+0yHYdRiCe4/aT5zOAprClYPsw2ZLAJdjxrYXgfJrnudxIei93s/rUJcUCvaT4Esp3bSU7+nQK9aMb7lHyCGhaDJNC
n7c+ylcxCNeaq54QQmi1OQlo2Kvvq8iSrjh/D2mgSJ02iKiYOiJM28GtQ2csRgQSduflviN9a5fb5TdGvgBA==
X-YMail-OSG: 3.j.g34VM1kfruyqKA_wVA39FA6bG74nIIdq4w1kAWS66KTCaC_nrBBOGqMEuDa
 JpRDkm2ebf7Eb.i.vPl.odVLcU0vIb0zWpLYW3c8tePXwfOGUrv3QYcYizcX31JC2i4ld4bdBwoN
 Ed6tJkHH39LCszcxu_u64IlRC4Avxu6RvWnjmxrmt3HLYWI5n6ODsZ1f_Edww4X51MVvm5cErbKk
 Ch4B6acgyNoS6_38f_IuMYAycHUMgBIFtC0wXYyJl7WJcRVGScuwsbFklymIZmJIGbYHc3XgWtSP
 A85n_851M16aegWOzNdBUxw2ZPhp3nM3TLl2mYltlnnSnaai97nqlUatRuzcob6_OXUpxAdvnck7
 UKcIg.It66a5mD_xqEDUe1h0k0pICNKED5SAR7HGdsYT4IcKnzImnz8p.Y2pIgfQDFrHqos1Q2aG
 CpfuCCqMroRx4ZjoC7u7oaAi3nHCMmxOsomjEWXf_bFC8WIGZpd2FuxhLmesvnByGAj0WcFRFsLA
 Yjh7YmNdFHC_jlNkRmQCCGX7yzcetpIADHDKf3LFaaLnuiRF1KyfaaKhuZim7HFCnVuGMtIKm9Vl
 nIBHZvTJCenxsScQ4ziizhNzXfHTucgRvjVobSY4hNpMtwWBIFF3IUMPuIWYEErGa8nw.R5U.Mch
 VSvSsN3w.tZOp3fFrzNH5kEM4xoYblHCTpywDTLDHTA7lHBMJfZ2KYN7wloeSTkcMV19CwP0qmEC
 0gdgs6X7ke4AaM8wowYGTpOg4TdvRKeuURHzCsn5bBi9nKKGq8AbZCaTdBbOlwntsEEkksh7KPVW
 iNm.DpUh7ZEQu6RNWfxCuqNrck8SpeTU32LH0z4LftAaUcRAZ8wqMUQTr7v9zyDoDNAN0H7lwb8L
 c1czADflxB6oLT66AJ0boZseWs78jExk4BO6dg2CRiiIlbJZ.B4B3_Dk4ZiN51Nwa_5BS5yrFpz.
 VH4ncRe_KyrSj2PtD8xdtWiplF22Kxo7VSaTbCZjii055fxPIbprmjOpT8PJkf0flHU_hEhuYdv7
 iZN0TJYHav91i8Id4OU0AM6suy9Nk_x0Kkk6gYfgGLaoV6iiVdTlmluWRAJJkjWzY2LCWJ1rbtXS
 iye5mxycKcWODr2mgtlEFIjVckB91r03C9_aM1.QtLiCaYSB9IBnTCg7Bb8WbS4t3bOQN3eglgUj
 C51ZoUEw2PT_0Wv.JQ0Xs7TO1OQ42egeowOwpdVybMOeTYYeuz77CagaA6g--
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.bf2.yahoo.com with HTTP; Mon, 15 Jul 2019 19:00:40 +0000
Date: Mon, 15 Jul 2019 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="----=_Part_915725_248640444.1563217119409"
References: <660010183.915726.1563217119410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.13991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700
X-CMAE-Envelope:
MS4wfLZlB7CaMDrryNg4bKn55ydjUqDKCWBS9G3ok/BIKlkU8Zlsy82e/vSUfOmU7oimgtG0yXPVpfsC1jxBMM4BNLz+MoWQBwtojDPEZQwRhUYMcwWoZEfb
 hxr2yJFh5Lub21K8mK/Y6fcDSXBHSrgLz4rcKsXyk2+zTyPEFo9DbH7mP2wiSAuCTxUPs47+Hj710A==
X-Nonspam: None

------=_Part_915725_248640444.1563217119409
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

Hello,
Please proceed with the transaction immediately. Thank you.

------=_Part_915725_248640444.1563217119409
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-
size:16px;"><div dir="ltr" data-setdir="false">Hello,</div><div dir="ltr" data-setdir="false"><br></div><div dir="ltr" data-
setdir="false">Please proceed with the transaction immediately. Thank you.<br></div></div></body></html>
------=_Part_915725_248640444.1563217119409--
```

- For example hidden timestamps within email source

- **Timestamps in the X-Received Header**
- `X-Received: by 2002:adf:eb48:: with SMTP id u8-v6mr18710230wrn.22.1541439809490;`
- SMTP ID contains an Epoch timestamp representing Monday, November 5, 2018 5:43:29.490 PM (UTC).

- **Timestamps in MIME Boundary Delimiters**
- `----=_Part_915725_248640444.1563217119409--`
- Epoch timestamp representing Monday, July 15, 2019 6:58:39.409 PM (UTC).

- **Timestamps in the Message-ID and References Header Fields**
- `Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>`
- `References: <660010183.915726.1563217119410.ref@mail.yahoo.com>`
- Epoch timestamps that read Monday, July 15, 2019 6:58:39.410 PM (UTC).

Short break – 5 mins

And then Week 2 part 3:

- Explain tutorial/lab
- Explain Major Assignment(assessed)