SWINBURNE UNIVERSITY OF TECHNOLOGY

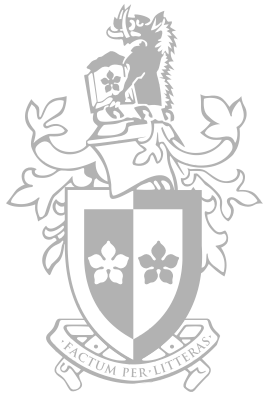
ICT30010 eForensic Fundamentals

Lecture 9

Time zones and Time lines

Troy Pretty

Digital Forensic Analyst



SWINBURNE UNIVERSITY OF TECHNOLOGY

Lecture Outline

- Time zones
- Time lines
- Event sources

Time Zone Types

- Many different ways to describe time zones
  - Greenwich Mean Time (GMT)
  - Coordinated Universal Time (UTC)
  - Zulu Time (Z Time)
- Each have different origins

Time Zone Types

- For the purpose of digital forensics their backgrounds have no effect
- Each can be interchanged to mean the same thing
- Will mainly see GMT or UTC

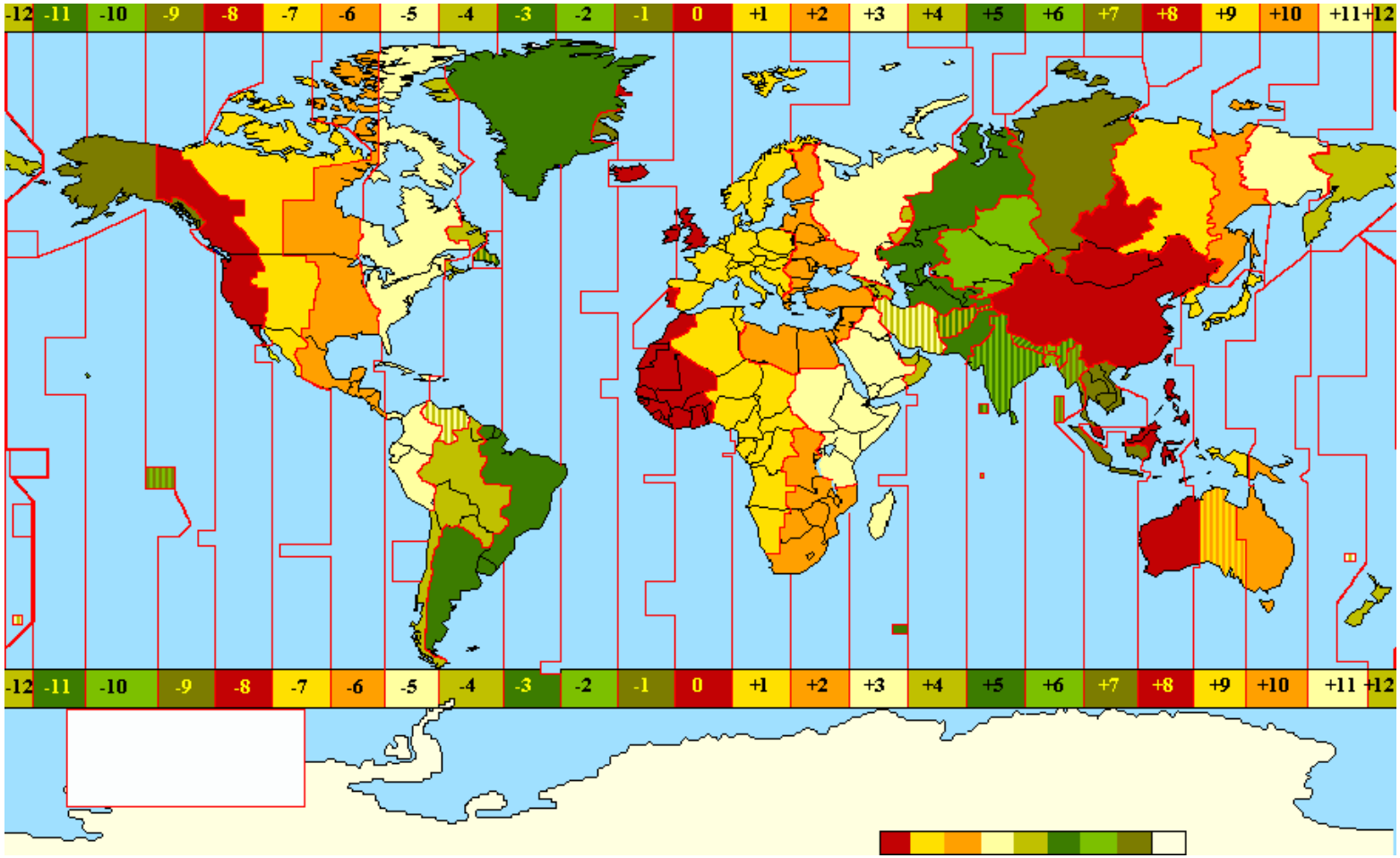
Time Zones

- GMT or UTC refers to the time at the Prime Meridian
  - Longitude 0 degrees
  - Greenwich, England
- Time zones represent the time offset from GMT/UTC
  - - hours behind GMT/UTC
  - + hours ahead of GMT/UTC
  - Each 15 degrees east or west represents a shift of 1 hour

Time Zones

- In theory there should be 24 different time zones
  - 1 for each hour in the day
  - In fact there are more
    - Some time zones are only 30 or 45 minutes apart
    - Daylight savings time adds additional time zones

Time Zone Map



Source: http://www.statsagogo.com/timezone

Time Zone Display

- Time zones can be displayed in different formats
  - UTC
  - GMT + 10
  - UTC -8
  - PST
  - Australia/Melbourne
- Need to know how to identify and understand

Time Zone Conversion

- When conducting forensic investigations its not uncommon to come across logs in different time zones depending on their source
- Check analysis computer date, time, time zone
- Check time zone on exhibits and adjust
- Convert all logs to a consistent format
  - Local time
  - UTC

Time Zone Conversion

- Manually convert times
  - 02/05/2018 0400 UTC
    - Need to add 10 hours to get to AEST (UTC +10)
    - 02/05/2018 1400 UTC +10
  - 02/05/2018 0400 UTC -8
    - Need to add 18 hours to get to AEST (UTC +10)
    - 02/05/2018 2200 UTC +10
- Websites can assist
  - https://www.timeanddate.com/worldclock/converter.html

Time Zone Considerations

- Depending on the time and time zone after conversion the date could change
  - The evening of UTC -8 will become the afternoon of the next day when converted to +10
- Daylight savings time can results in the same time being logged with a different time zone
  - 2 am AEDT (UTC +11)
  - 3 am AEDT (UTC +11)
  - 2 am AEST (UTC +10)
  - 3 am AEST (UTC +10)

Time Lines

- Important tool in a forensic investigation
- Used to paint a holistic picture of the events relevant to an investigation
- Not sufficient for evidence to simply be on a computer
  - Need to show intent
  - Need to show how it come to be on a computer

Time Line Creation

- Manual Tools
  - Specific to a particular event
  - Helps paint a specific picture
  - Easy to read and understand
  - IE. Flow charts

Time Line Creation

- Automated tools
  - Process all dates and times on a computer
  - Takes a long time
  - Produces massive reports with lots of irrelevant information
  - Autopsy time – File system access
  - Timescanner Super Timeline
    - Internet history
    - Event logs
    - Etc

Time Line Pivoting

- Start with a known event
  - Website access
  - Hacking Event
- Look at events either side of the known event
  - Drill down on dates/times of interest
  - Attempting to locate unknown events
  - Helps to show intent
  - Helps to understand what has occurred

Event Sources

- Local Devices
  - Computers
  - Phones
  - Storage Devices
- Logs provided from 3rd parties
  - Service providers
  - Victim servers

Event Sources

- Other Sources
  - CCTV
  - Door access
  - Phone records
  - Bank records
- Think outside the box, don't just focus on the digital devices

Interesting Digital Events

- Windows Event Logs
  - PC power on/shutdown
  - User logon/logoff
  - Software install
  - Date/Time changes

Interesting Digital Events

- Internet History
  - Websites visited
  - Search terms
  - Also logs local files opened via windows explorer

Interesting Digital Events

- Recycle Bin / INFO2 Records
  - Files deleted
  - Date/Time
  - Original location

Interesting Digital Events

- Windows Prefetch
  - Built-in windows function to speed up applications
  - Files cached to disk
  - Can indicate when an application is first run

Interesting Digital Events

- Windows Link (LNK) files
  - Shortcuts to application files
  - User created (i.e.. Desktop)
  - Created by application installs
  - “Recent Files” created when files are opened
    - Good indication that file has been viewed/accessed

Interesting Digital Events

- Chat / Email
  - Good evidence to put a person in front of computer
    - Communications
    - Planning
    - Bragging

Interesting Digital Events

- File System
  - Downloading files
  - Installing applications
  - Creating documents
  - Attachments from chat/emails

Summary

- Time zones
- Time lines
- Event sources