Digital Forensics

An introduction

VC2TDI10S01: investigate how hardware and software manage, control and secure access to data in networked digital systems

VC2TDI10D011: investigate simple data compression techniques

Learning Intention and Success Criteria

Learning Intention:

Students will learn the basics of digital forensic investigations, and different ways data is secured on a computer

Success Criteria:

Students will understand the process of a digital forensic investigation, how HTML can be inspected and how base64 is used to encode data, and some basic cryptographic methods

Cyber Crime

- *Question*: What is it?

- Cybercrime is one of that fastest growing crime types in Australia with hundreds of millions of dollars lost each year.

- Cybercrime is often linked to:
  - Drug crime
  - Fraud and corruption
  - Money laundering/financial crime
  - Serious and organised crime

Cyber Crime

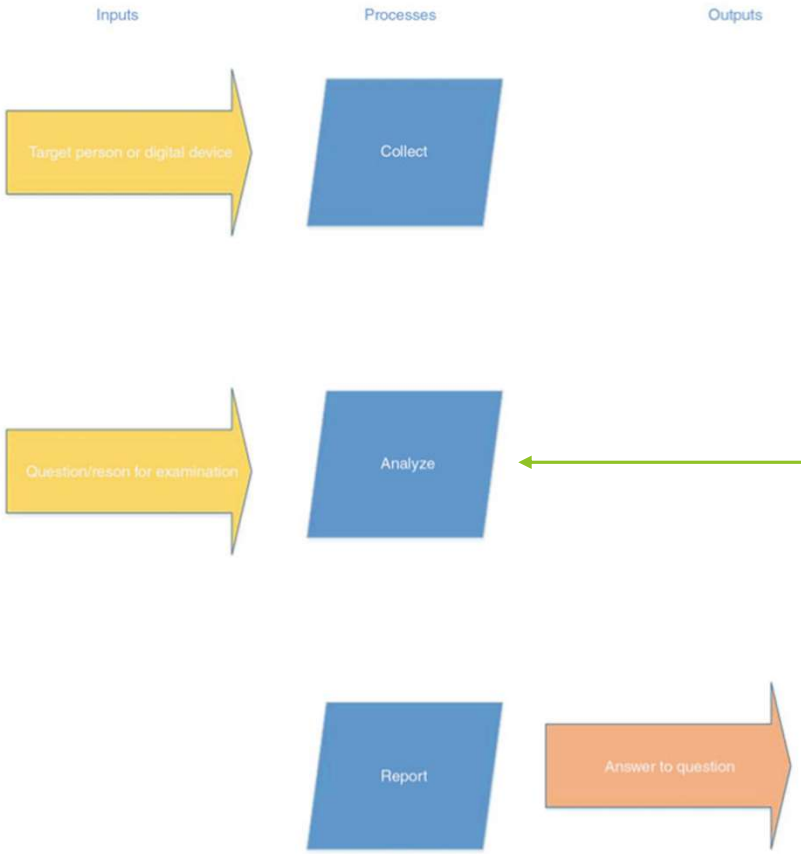
- Let's say the police have a warrant to seize and search a computer of a known criminal. How do we find investigate it?

- By using **digital forensics**

Digital Forensics: What is it?

- *"the examination of digital storage and environments in order to determine what has happened"*
  - "What has happened", in this context could be anything! For example:
    - whether a crime was committed
    - whether someone remote controlled a certain computer
    - when a picture was taken
    - if a computer was subject to intrusion

The Forensic Process



Analysis will be our focus

Analysis: Hard Drives

- When we have access to a suspect's hard drive, we use a tool like **FTK Imager** to analyse it.
- This creates a bit-by-bit copy of a hard drive, USB, etc.
- The program then allows us to:
  - View contents of the drive without deleting them
  - Recover deleted files
  - Analyse meta-data (timestamps, when files were created or modified, etc.)

Analysis: Photos

- Every digital photo taken stores ‘metadata’ within the image file.
  - This is called **EXIF data**
- This includes things like:
  - Date photo was taken
  - The camera it was taken on
  - GPS coordinates of where it was taken
  - And many more

Analysis: Photos

- We can use digital tools to extract this data. For example, **EXIFtool**
- This can be very useful in forensic investigations to determine things like timelines of events, and locations of individuals

Analysis: Web Files

- Web sites are commonly structured using ‘HTML’
- It is all about **organizing and displaying information** on a webpage
- It is a markup language, **not** a programming language
  - It annotates text to define how it is structured by web browsers
  - It *does not* perform calculations or logic

Analysis: Web Files

- Whilst HTML does *not* reveal actual source code, it can reveal clues to how things work behind the scenes, creating vulnerabilities

- Example:
  - A developer leaves a ‘comment’ in their code they forget to remove. This can unintentionally expose information not meant for the public

Analysis: Web Files

- How it's done:

1. Go to a web browser
    - For windows – click : CTRL + SHIFT + I
    - For Mac - click: Option + Command + I

2. Go to the elements tab to look through the HTML

https://www.mozilla.org/en-GB/?v=c

Cryptography: how to hide data

- Cryptography hides information so that only the person that a message is intended for can read it.
- It goes all the way back to ancient Egyptians.
- The fundamental application of cryptography is **encryption**

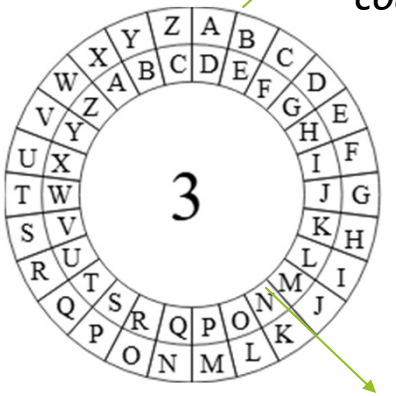
Encryption and Decryption

- **Encryption** is how we conceal the messages.
- One of the simplest methods of encryption is called the **Caeser cipher.** (named after Julius Caeser)
- How it works:
  - Define a 'Shift', e.g. shift = 3, and direction, e.g. right (*Only the creator and receiver know this)*
  - Each letter in the alphabet shifts 3 spaces that direction
  - To **decrypt,** shift the letters back 3 in the opposite direction

Encryption and Decryption: Caeser Cipher

Message: Hey Everyone

Encrypted Message: Ebv bsbovlkb



Outer circle has ‘shifted’ 3 places left (*or counterclockwise)*

The inner circle is the original, and the outside will be what each letter becomes when encrypted

Cryptography: Steganography

- Steganography is a form of cryptography where information is hidden within another message or physical object
- This can be applied digitally, by hiding a file within another file. For example:
  - Placing a message within an image
- *Extension Question*: what is the advantage of this over encryption alone?

Cryptography: Steganography

- It is often combined with encryption for extra security
- One method of steganography:
  - Adjust the colour of every 100th pixel to correspond to a letter in the alphabet
  - *This change is so subtle, someone who is not looking for it is unlikely to notice*
- We can use online websites to decipher images we may think have hidden messages within them. E.g. https://stylesuxx.github.io/steganography/