CS4HS 2022 …Cracking…Forensics...

Alastair Nisbet anisbet@aut.ac.nz

- There are 2 practical demonstrations
- Linux – Kali
- Cracking a password using ‘pdfcrack’
- Making an image of a usb stick
- and then recovering deleted files using ‘foremost’

CS4HS 2022
…Cracking…Forensics…

- A PDF file is encrypted with a password
- Passwords are minimum of 4 – 6 characters
- 26 letters in the alphabet
- Uppercase and lowercase = 52 possible characters
- A number is also permitted = 10 possible numbers
- Total of 62 possible characters
- 62^6 = 62x62x62x62x62x62=56,800,235,584
- Divided by 50,000 = 1,136,004 (seconds to try all)
- = 315 hours or almost 2 weeks

CS4HS 2022
…Cracking…Forensics…

- If we know that the password only contains lowercase characters
- 26^6 = 308,915,776 possible passwords
- Divided by 50,000 = 6178 seconds
- About 1 hour and 45 minutes to crack
- Characters lowercase a – m (18 characters)
- 18^6 = 34,012,224 / 50,000 = 680 seconds
- Just over 11 minutes to crack

CS4HS 2022 …Cracking…Forensics…

- Image the usb stick (/dev/sdb in this case)
- dcfldd if=/dev/sdb of=Desktop/cs4hs.dd hash=md5 conv=sync,noerror
- Hash the stick to get the MD5 hash
- Take the image – cs4hs.dd
- Hash the image >md5sum Desktop/cs4hs.dd
- Compare hashes
- If they match – the file and usb stick have identical data – every 0 and 1 is the same

CS4HS 2022
…Cracking…Forensics...

- Use Foremost to recover files from the image
- Dcfldd Desktop/cs4hs.dd –o Desktop/cs4hsfiles
- Foremost creates folders first, looks for files and then deletes empty folders
- Foremost is quick and simple but looks for limited types of files
- The name of the file is the ‘inode’ address (where the file is located on the usb stick or image)