# C.I.A TRIAD

# CONFIDENTIALITY

Confidentiality is about ensuring access to data is restricted to only the intended audience and not others. As you may expect, the more sensitive the information is, the more stringent the security measures should be. Many privacy laws rely on confidentiality security controls to enforce legal requirements.

Example:

- Encryption
  - **sudo apt install gnupg → gpg –c file → gpg file.gpg**
- 2FA or MFA
- Password protect
- Biometrics

# INTEGRITY

**Integrity** refers to maintaining the accuracy, and completeness of data. In other words, it is about protecting data from being modified by unauthorized parties, accidentally by authorized parties, or by non-human-caused events such as electromagnetic pulse or server crash. For example, a hacker may intercept data and modify it before sending it on to the intended recipient.

**From PowerShell:**

**Get-FileHash filename.txt**

**From Kali:**

**md5sum filename.txt**

**sha1sum filename.txt**

**sha256sum filename.txt**

# AVAILABILITY



**Availability is ensuring** information must be available when it is needed. To ensure high data availability, you must maintain a correctly functioning hardware and software and provide adequate bandwidth.

**Example:**

**- Off-site backup**

**- Disaster recovery**

**- Failover**

# On Kali Linux

## Are these 2 images the same or different?

# STEGANOGRAPHY



**What is Steganography?**

Steganography is the practice of concealing a message or information within another file, image, or medium in a way that makes it difficult to detect.

# STEGANOGRAPHY HISTORY



Steganography was created to address the need for covert communication and the concealment of information.

## Military and Espionage Purposes:

Throughout history, steganography has been used in warfare and espionage to exchange confidential messages without alerting enemies or adversaries.

In ancient Greece, military commanders used shaved heads, tattoos, and regrown hair to hide messages.

# Covert Communication:

In various covert and intelligence operations, steganography is a valuable tool for **securely transmitting classified** or sensitive information between agents or organizations.

## Protection of Intellectual Property:

Steganography is used to embed digital watermarks, copyright information, and ownership details in digital media such as images and videos to protect intellectual property and prove ownership.

## Cybersecurity and Malware:

In the digital age, steganography has been used in cyberattacks to hide **malware**, command-and-control instructions, or stolen data within files. This technique is used by cybercriminals to **evade** detection and carry out their activities covertly.

## Data Transfer:

Steganography is employed when individuals or entities need to **transfer data discreetly**, whether for legitimate or security-related purposes.

# Types of Steganography

# IMAGE STEGANOGRAPHY



Hiding Messages in Images

# AUDIO STEGANOGRAPHY



Concealing Data in Sound

# TEXT STEGANOGRAPHY



Hidden Messages in Text

# INSTALL STEGHIDE ON KALI



```
# sudo apt install steghide
```

## EMBED DATA

```
# steghide embed –ef secret.txt –cf pic1.jpg –p beriteck
```

## EXTRACT DATA

```
# steghide extract –sf pic1.jpeg –p beriteck –xf xsecret.txt
```

# MORE STEGANOGRAPHY COMMANDS



**1. Embed data in a PNG, prompting for a passphrase:**

```
# steghide embed --coverfile path/to/image.png --embedfile
path/to/data.txt
```

**2. Extract data from a WAV audio file:**

```
# steghide extract --stegofile path/to/sound.wav
```

**3. Display file information, trying to detect an embedded file:**

```
# steghide info path/to/file.jpg
```

**4. Embed data in a JPEG image, using maximum compression:**

```
# steghide embed --coverfile path/to/image.jpg --embedfile
path/to/data.txt --compress 9
```