

# CTF на Физтехе

Занятие 7

# Стеганография

# Стеганография

- Способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения)
- Сообщение не привлекает к себе внимания
- Стеганография + криптография = <3

# Классика

- Симпатические (невидимые) чернила
- Микроточки (микро изображения)
- Татуировка на голове раба

# Пример

- Adrian: Todd told April Carmen Kelly and Trent. Daniel Arkum was not moving out now. Daniel's awaiting you.

# Пример

- Adrian: Todd told April Carmen Kelly and Trent. Daniel Arkum was not moving out now. Daniel's awaiting you.
- ATTACK AT DAWN MONDAY

# Основные понятия

- Сообщение - передаваемая скрытая информация
- Контейнер - информация, используемая для сокрытия сообщения

# Компьютерная стеганография

- Основана на особенностях компьютерной платформы
- Контейнеры
  - Служебные поля форматов файлов
  - Неиспользуемое пространство диска
  - Встраивание информации путем внесения незначительных искажений, невоспринимаемых человеком



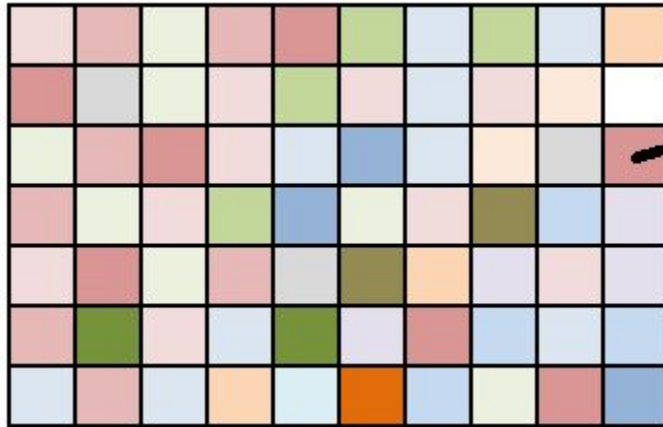
# Изображения

- EXIF метаданные
- Изменение палитры
- Внесение искажений
  - Незаметные цвета
  - Least Significant Bit

# Least Significant Bit

- Least Significant Bit (LSB) - наименьший значащий бит
- Замена последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения
- Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека

# Least Significant Bit



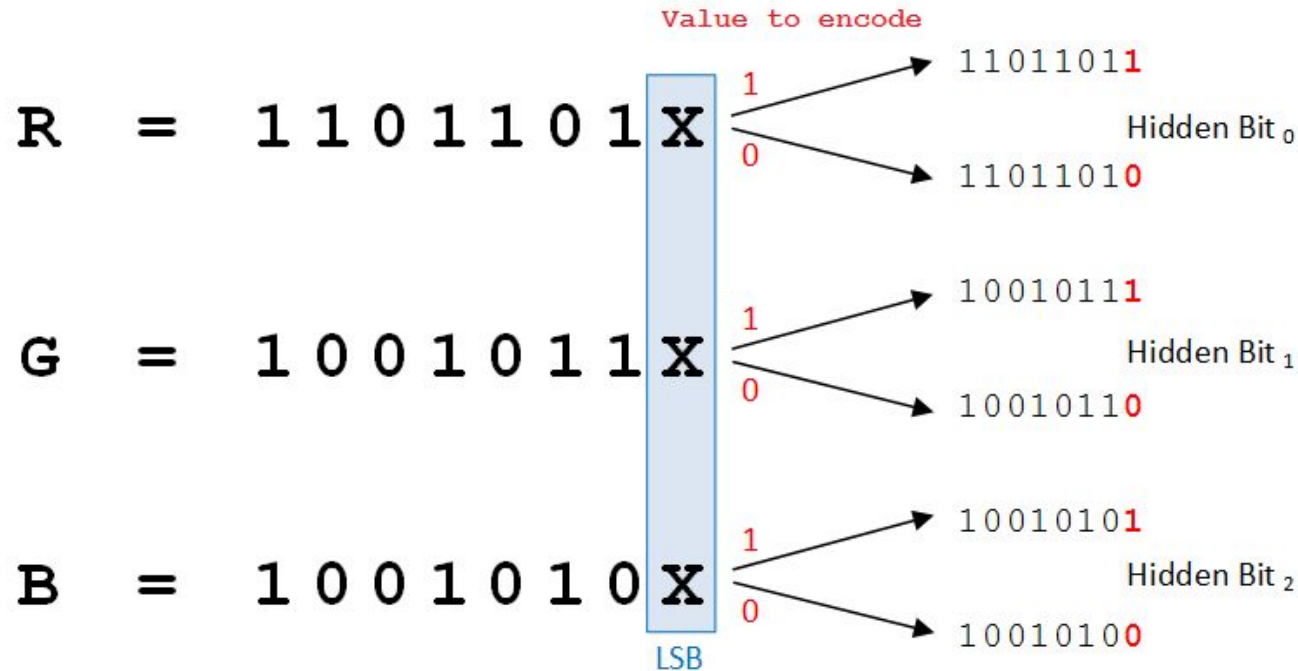
RGB (218, 150, 149)

R = 11011010


G = 10010110

B = 10010101

# Least Significant Bit



# Least Significant Bit

Hex	Red: Int	Red: Bin	Color
#3fff16	63	0b00111111 <b>1</b>	
#3eff16	62	0b00111111 <b>0</b>	

# Least Significant Bit: пример



- <https://github.com/luca-m/lbs-toolkit>

# Least Significant Bit

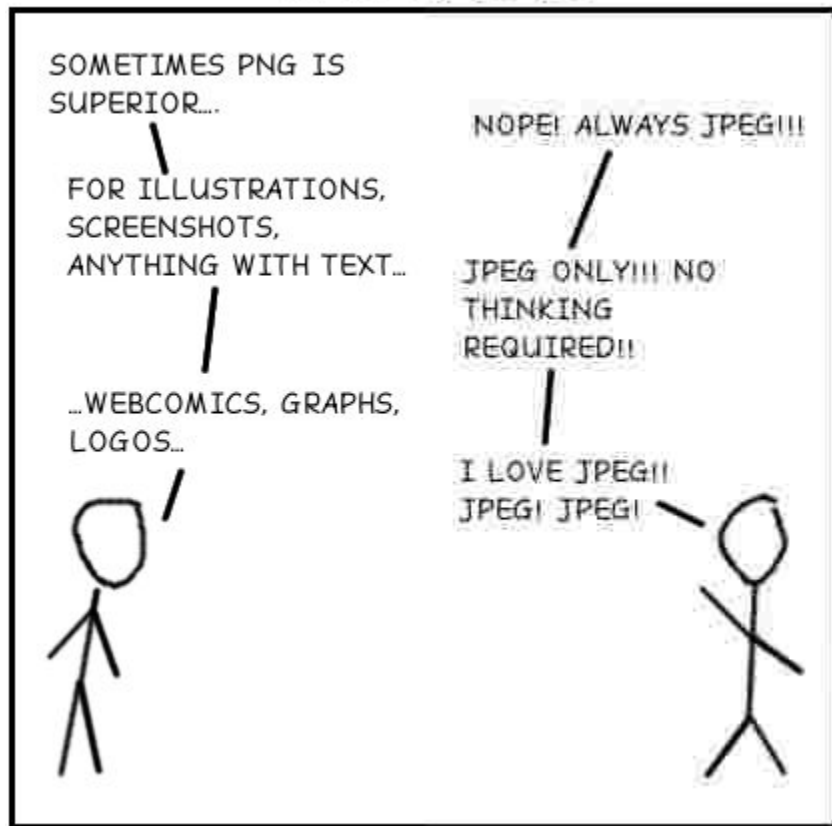
- LSB для значений цветов пикселей работает лишь для некоторых форматов (PNG, BMP, ...)
- Формат JPEG устроен по другому

**JPEG**



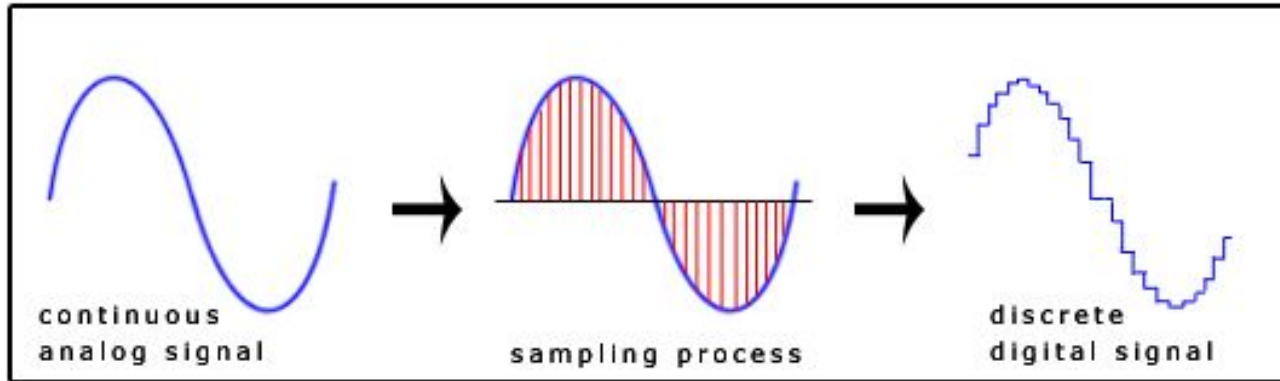
# PNG vs JPEG

PNG vs JPEG



# Аудио

- Метаданные
- LSB для значений амплитуд



- Работает для WAV
- MP3 устроен сложнее

# Другие форматы файлов

- Необходимо детальное понимания того, как работает конкретный формат
- Видео ~= изображение + аудио
- Пример: jpeg + rar

# Стегоанализ

- Атака на стегосистему - попытка обнаружить, извлечь, изменить скрытое стеганографическое сообщение
- Типы атак:
  - Атака по известному заполненному контейнеру
  - Атака на основе известного пустого контейнера
  - ...

# Применения

- Желтые точки при печати на принтере
- Цифровые водяные знаки (Watermarks)
- Спецслужбы?
- Террористы?
- CTF

# Инструменты

- Изображения
  - ExifTool
  - Python + Python Imaging Library (PIL)
  - Stegsolve
  - <https://tineye.com/>
- Звук
  - Audacity
  - Sonic Visualiser

**Вопросы?**