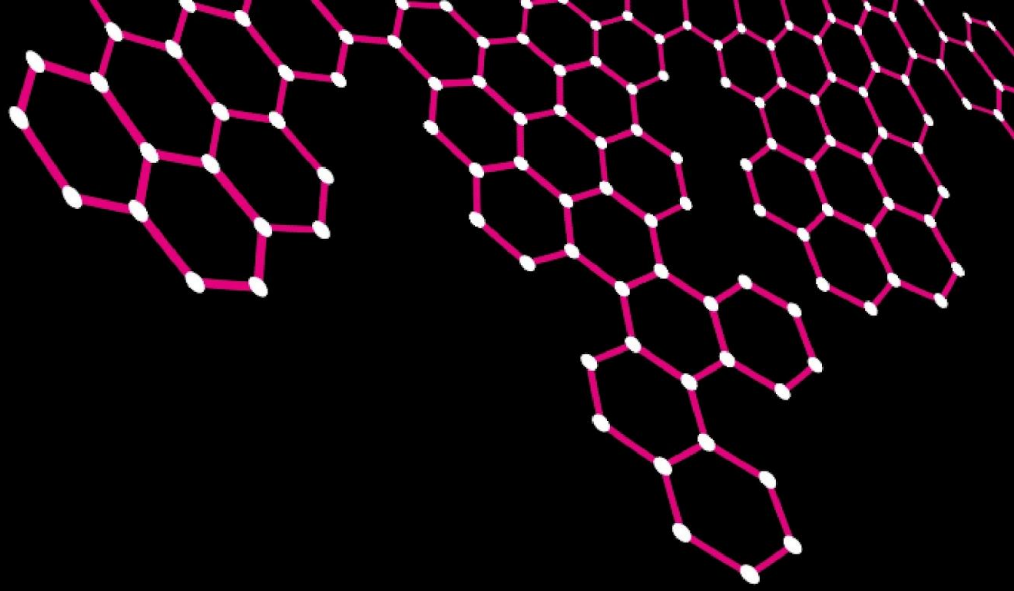
UNIVERSITY OF TWENTE.



THS - Forensics

Including Steganography & OSINT

Thijs van Ede (t.s.vanede@utwente.nl)

Forensics

- Track breadcrumbs left by an attacker

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”
    - Are there still traces left in the memory?

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”
    - Are there still traces left in the memory?
  - Is a file completely anonymized?

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”
    - Are there still traces left in the memory?
  - Is a file completely anonymized?
    - Does it still contain meta-data?

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”
    - Are there still traces left in the memory?
  - Is a file completely anonymized?
    - Does it still contain meta-data?
    - Did a program unexpectedly change other files, leaving traces of data?

Forensics

- Track breadcrumbs left by an attacker
  - Traces that an attacker (incidentally) leaves behind
  - Requires knowledge about the workings of many different commonly used programs
  - Simple example, when you delete a file:
    - Is it still in the trash bin?
    - Are the actual bytes overwritten on the disk, or is it simply marked as “Can overwrite in future?”
    - Are there still traces left in the memory?
  - Is a file completely anonymized?
    - Does it still contain meta-data?
    - Did a program unexpectedly change other files, leaving traces of data?
  - You will get a feeling for this with practice!

Steganography

- Hiding messages within other non-suspicious looking data

Steganography

- Hiding messages within other non-suspicious looking data
- By changing bits of a in such a way that humans will not notice, we can encode data

Steganography

- Hiding messages within other non-suspicious looking data
- By changing bits of a in such a way that humans will not notice, we can encode data
- Example, hiding data in images:

Steganography

- Hiding messages within other non-suspicious looking data
- By changing bits of a in such a way that humans will not notice, we can encode data
- Example, hiding data in images:
  - Image files encode the RGB values of each pixel as a 8-bit number.

Steganography

- Hiding messages within other non-suspicious looking data
- By changing bits of a in such a way that humans will not notice, we can encode data
- Example, hiding data in images:
  - Image files encode the RGB values of each pixel as a 8-bit number.
  - If we change the least significant bit of each number, we can encode data, but the picture will not change much visually

Steganography

- Hiding messages within other non-suspicious looking data
- By changing bits of a in such a way that humans will not notice, we can encode data
- Example, hiding data in images:
  - Image files encode the RGB values of each pixel as a 8-bit number.
  - If we change the least significant bit of each number, we can encode data, but the picture will not change much visually
- Often, data is hidden within images, sound files, or other files where small changes in the encoding will not break the file itself

OSINT

- Use open source intelligence to find the flag

OSINT

- Use open source intelligence to find the flag
- Track people, organizations, or flags stalking them on the internet / social media

OSINT

- Use open source intelligence to find the flag
- Track people, organizations, or flags stalking them on the internet / social media
  - Not very common for CTF challenges, but is common for real world hacking/social engineering

OSINT

- Use open source intelligence to find the flag
- Track people, organizations, or flags stalking them on the internet / social media
  - Not very common for CTF challenges, but is common for real world hacking/social engineering
- Try searching public datasources:

OSINT

- Use open source intelligence to find the flag
- Track people, organizations, or flags stalking them on the internet / social media
  - Not very common for CTF challenges, but is common for real world hacking/social engineering
- Try searching public datasources:
  - Google
  - Facebook
  - Twitter
  - Instagram
  - Etc.

Let’s start hacking

- Challenges
  - See https://ths.eemcs.utwente.nl/resources
- Tools:
  - binwalk
  - steghide
  - wireshark

UNIVERSITY OF TWENTE.