



# IDENTIDAD Y FORENSIA

**Jess Garcia** - Fundador y CEO de One eSecurity

- Instructor Senior SANS Institute

[jess.garcia@one-esecurity.com](mailto:jess.garcia@one-esecurity.com)

Twitter: [@j3ssgarcia](https://twitter.com/j3ssgarcia)



**Jess García**

[jess.garcia@one-esecurity.com](mailto:jess.garcia@one-esecurity.com)

[@j3ssgarcia](#)



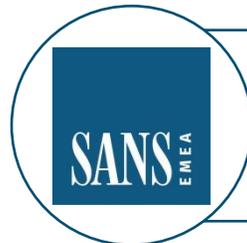
**Fundador y CEO de One eSecurity**  
**25+ años de experiencia en CybSec / DFIR**



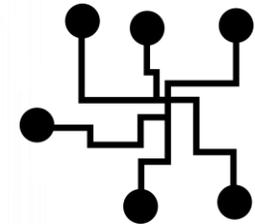
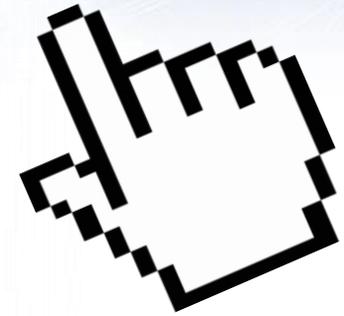
**Compañía global de DFIR de 16+ años**  
[www.one-esecurity.com](http://www.one-esecurity.com)



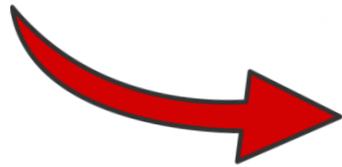
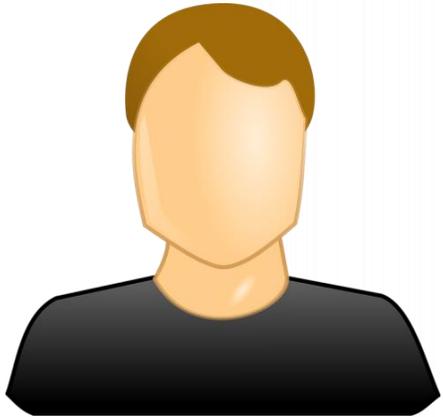
**Líder del proyecto DS4N6**  
[www.ds4n6.io](http://www.ds4n6.io)



**Senior Instructor en SANS Institute**  
**20+ años**



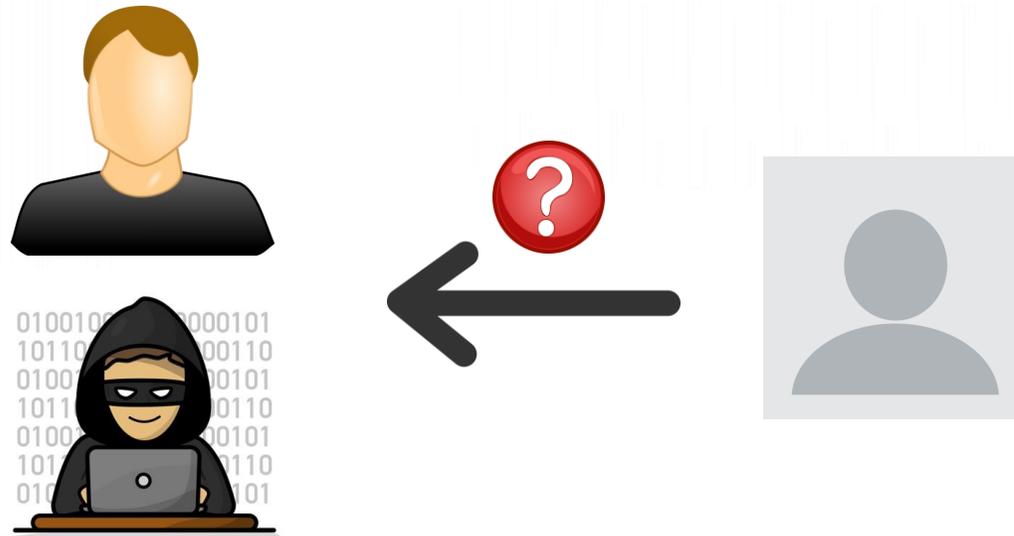




# </Identidad en procesos legales>



Escenario por defecto  
**IDENTIDAD = PERSONA**



Escenario alternativo  
**IDENTIDAD != PERSONA**



# </Caso de estudio real>

# La búsqueda de la Identidad



Empleado descontento



Acceso a información  
confidencial de RRHH

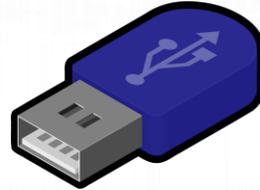


Distribución anónima de  
información

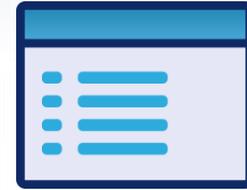
# </Análisis forense de artefactos>



**Browser Activity**



**External Device/USB Usage**



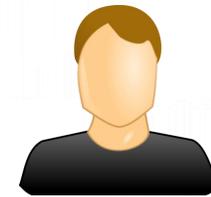
**Application Execution**



**Network Activity**



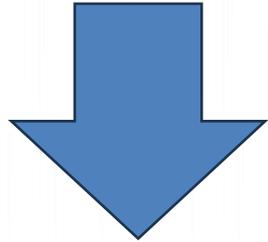
**File and Folder Opening**



**Account Usage**

<https://www.sans.org/posters/windows-forensic-analysis/>

## Forense del servidor vulnerado

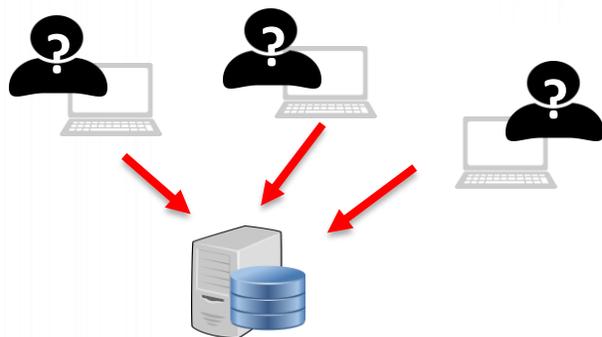


- Usuario legítimo de HR comprometido
- IPs de ordenadores en salas de reuniones
- Tiempos de la actividad maliciosa

## EVENT LOGS

- Security Event Log – security.evtx
  - 4624 Logon Type 3
    - Source IP/Logon User Name
  - 4672
    - Logon User Name
    - Logon by user with administrative rights
    - Requirement for accessing default shares such as c\$ and ADMIN\$
  - 4776 – NTLM if authenticating to Local System
    - Source Host Name/Logon User Name
  - 4768 – TGT Granted
    - Source Host Name/Logon User Name
    - Available only on domain controller
  - 4769 – Service Ticket Granted if authenticating to Domain Controller
    - Destination Host Name/Logon User Name
    - Source IP
    - Available only on domain controller
  - 5140
    - Share Access
  - 5145
    - Auditing of shared files – NOISY!

Map Network Shares (net.exe) to C\$ or Admin\$



192.168.1.100

<https://www.sans.org/posters/hunt-evil/>

[www.one-esecurity.com](http://www.one-esecurity.com) | [www.ds4n6.io](http://www.ds4n6.io)

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: SYSTEM
- Account Name: WIN-GG82ULGC9GOS
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:

- Logon Type: 2
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: CONTOSO\Administrator
- Account Name: Administrator
- Account Domain: WIN-GG82ULGC9GO
- Logon ID: 0x8DCDC
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Event Properties - File: E:\C\Windows\system32\winevt\logs\Sec...

Standard XML

|                    |   |           |                                     |
|--------------------|---|-----------|-------------------------------------|
| Date:              | 9/5/2018  | Source:   | Microsoft-Windows-Security-Auditing |
| Time:              | 12:02:15 PM   | Category: | Logon                               |
| Type:              | Audit Success   | Event ID: | 4624                                |
| User:              | N/A   |           |                                     |
| Computer:          | base-rd-01.shieldbase.lan   |           |                                     |
| Description:       | An account was successfully logged on.  |           |                                     |
| Subject:           | Security ID: S-1-5-18<br>Account Name: BASE-RD-01\$<br>Account Domain: shieldbase<br>Logon ID: 000003E7 |           |                                     |
| Logon Information: | Logon Type: 2   |           |                                     |

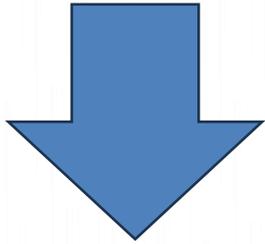
Event Properties - File: E:\C\Windows\system32\winevt\logs\Sec...

Standard XML

|              |  |           |                                     |
|--------------|--|-----------|-------------------------------------|
| Date:        | 5/11/2018  | Source:   | Microsoft-Windows-Security-Auditing |
| Time:        | 7:39:38 PM   | Category: | Logoff                              |
| Type:        | Audit Success  | Event ID: | 4647                                |
| User:        | N/A  |           |                                     |
| Computer:    | base-rd-01.shieldbase.lan  |           |                                     |
| Description: | User initiated logoff:   |           |                                     |
| Subject:     | Security ID: S-1-5-21-3445421715-2530590580-3149308974-1116<br>Account Name: tdungan<br>Account Domain: shieldbase<br>Logon ID: 001D7380           |           |                                     |
|              | This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event. |           |                                     |

## </Caso de estudio – Expandimos la búsqueda>

### Forense de los ordenadores de las salas de reuniones



- Usuario local genérico para entrar en el equipo
- Trazas de las conexiones al servidor donde estaba la información confidencial
- Multitud de IDs de dispositivos USB conectados

## Volume Serial Number

### Description

Discover the Volume Serial Number of the Filesystem Partition on the USB. (NOTE: This is not the USB Unique Serial Number, which is hardcoded into the device firmware.)

### Location

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt
- Use Volume Name and USB Unique Serial Number to:
  - Find last integer number in line
  - Convert Decimal Serial Number into Hex Serial Number

Editor del Registro

Equipo\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\??\_USBSTOR#Disk&Ven\_General&Prod\_UDisk&Rev\_5.00#6&3996b4c2&0&\_&0#{53f56307-b6b...

- > Accessibility
- > AdaptiveDisplayBrightness
- > AeDebug
- > AppCompatFlags
- > ASR
- > BackgroundModel
- > ClipSVC
- > Compatibility32
- > Console
- > Containers
- > CorruptedFileRecovery
- > DefaultProductKey
- > DeviceDisplayObjects
- > DiskDiagnostics
- > drivers.desc
- > Drivers32
- > EFS
- > EMDMgmt
  - > \_??\_&Ven\_Unknown&Prod\_Unknown&SYSTEM\_1948233599
  - > \_??\_USBSTOR#Disk&Ven\_General&Prod\_UDisk&Rev\_5.00#6&3996b4c2&0&\_&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}USB\_3502742398
  - > \_??\_USBSTOR#Disk&Ven\_LGE&Prod\_USB\_Drive&Rev\_1100#AA00000000018037&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}USB\_Drive\_783224626
  - > \_??\_USBSTOR#Disk&Ven\_Samsung&Prod\_Flash\_Drive\_DUO&Rev\_1100#0355215080028291&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}SAMSUNG\_USB\_908445432
  - > \_??\_USBSTOR#Disk&Ven\_SanDisk&Prod\_Cruzer\_Blade&Rev\_1.27#4C530202411209102450&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\_3187723938
  - > FWVQANJFLEOQOS\_1747165125
  - > FWVQAUVALUY\_1186605118
  - > FWVQIAPBPPDDATA\_3496853041

## Volume Serial Number

Calculadora

Programador

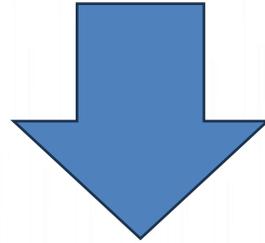
D0C7 9B7E

|     |               |
|-----|---------------|
| HEX | D0C7 9B7E     |
| DEC | 3.502.742.398 |

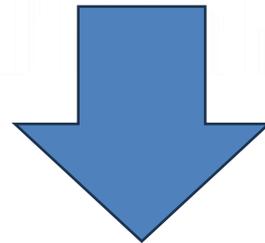
Volume Name: **USB**

## Análisis de los dispositivos USB

Correlación temporal del ataque con los IDs de los USBs conectados



Búsqueda masiva de los IDs en todos los ordenadores de la empresa

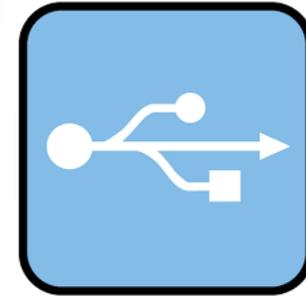


Gran número de hits por USBs chinos (IDs duplicados)

## </USB Footprint>



WINDOWS REGISTRY HIVES



SETUPAPI.DEV.LOG (PLUG AND PLAY LOGS)

# </USB Footprint – No encaja!>

Primera Conexión

C:/Windows/inf/setupapi.dev.log

USB Unique Serial Number

```
setupapi.dev.log
C: > Windows > INF > setupapi.dev.log
48410
48411 >>> [Device Install (Hardware initiated) - SWD\WPDBUSENUM\??_USBSTOR#Disk&Ven_General&Prod_UDisk&Rev_5.00#6&1e768de5&0&_&0#{53f56307-b6bf-11d0-94f2-00a0c91ef
48412 >>> Section start 2020/12/04 10:34:46.097
48413 utl: {Select Drivers - SWD\WPDBUSENUM\??_USBSTOR#Disk&Ven_General&Prod_UDisk&Rev_5.00#6&1e768de5&0&_&0#{53f56307-b6bf-11d0-94f2-00a0c91ef
48414 utl: Driver Node:
48415 utl: Status - Selected
48416 utl: Driver INF - wpdfs.inf (C:\WINDOWS\System32\DriverStore\FileRepository\wpdfs.inf_amd64_1183fd0f13045f2e\wpdfs.inf)
48417 utl: Class GUID - {eec5ad98-8080-425f-922a-dabf3de3f69a}
48418 utl: Driver Version - 06/21/2006,10.0.19041.746
48419 utl: Configuration - wpdbusenum\fs
48420 utl: Driver Rank - 00FF2000
48421 utl: Signer Score - Inbox (0D000003)
48422 utl: {Select Drivers - exit(0x00000000)} 12:34:46.137
48423 ! dvi: Device class {eec5ad98-8080-425f-922a-dabf3de3f69a} is not configurable.
48424 dvi: Searching for compatible ID(s):
48425 dvi: wpdbusenum\fs
48426 dvi: swd\generic
48427 dvi: Class GUID of device changed to: {eec5ad98-8080-425f-922a-dabf3de3f69a}.
48428 ndv: {Core Device Install} 12:34:46.172
48429 dvi: {Install Device - SWD\WPDBUSENUM\??_USBSTOR#DISK&VEN_GENERAL&PROD_UDISK&REV_5.00#6&1E768DE5&0&_&0#{53F56307-B6BF-11D0-94F2-00A0
48430 dvi: Device Status: 0x01802400 [0x01 - 0xc0000493]
48431 dvi: Parent Device: STORAGE\Volume\??_USBSTOR#Disk&Ven_General&Prod_UDisk&Rev_5.00#6&1e768de5&0&_&0#{53f56307-b6bf-11d0-94f2-00
48432 dvi: {DIF_ALLOW_INSTALL} 12:34:46.186
48433 dvi: Using exported function 'WpdClassInstaller' in module 'C:\WINDOWS\system32\wpd_ci.dll'.
```

## Mismo USB en 50 máquinas

Equipo\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven\_General&Prod\_UDisk&Rev\_5.00\6&1e768de5&0&\_&0

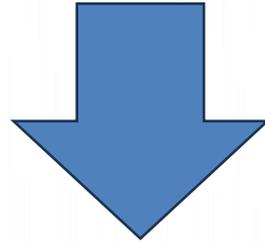
| Nombre           | Tipo         | Datos  |
|------------------|--------------|--|
| (Predeterminado) | REG_SZ       | (valor no establecido)                             |
| Address          | REG_DWORD    | 0x00000001 (1)                                     |
| Capabilities     | REG_DWORD    | 0x00000000 (0)                                     |
| ClassGUID        | REG_SZ       | {4d36e967-e325-11ce-bfc1-08002be10318}             |
| CompatibleIDs    | REG_MULTI_SZ | USBSTOR\Disk USBSTOR\RAW GenDisk                   |
| ConfigFlags      | REG_DWORD    | 0x00000000 (0)                                     |
| ContainerID      | REG_SZ       | {279ebc6b-1824-11ee-ba67-a0c5897bd5c1}             |
| DeviceDesc       | REG_SZ       | @disk.inf,%disk_devdesc%;Disk drive                |
| Driver           | REG_SZ       | {4d36e967-e325-11ce-bfc1-08002be10318}\0002        |
| FriendlyName     | REG_SZ       | General UDisk USB Device                           |
| HardwareID       | REG_MULTI_SZ | USBSTOR\DiskGeneral_UDisk_____5.00 USBST           |
| Mfg              | REG_SZ       | @disk.inf,%genmanufacturer%;(Standard disk drives) |
| Service          | REG_SZ       | disk   |

USB Unique Serial Number ID = **6&1e768de5&0&\_&0**

</Caso de estudio - Generando hipótesis>

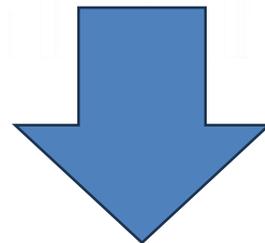
**Pregunta:**

**Cómo se comprometió ese usuario legítimo?**



**Hipótesis:**

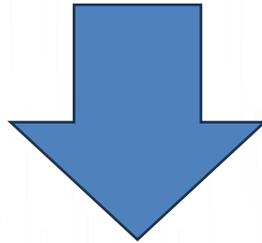
**Hacking / sniffing en un servidor intermedio**



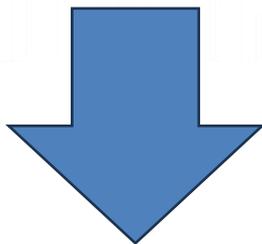
**Probablemente un usuario técnico**

</Caso de estudio - De vuelta al mundo real>

## Análisis de USBs de usuarios técnicos



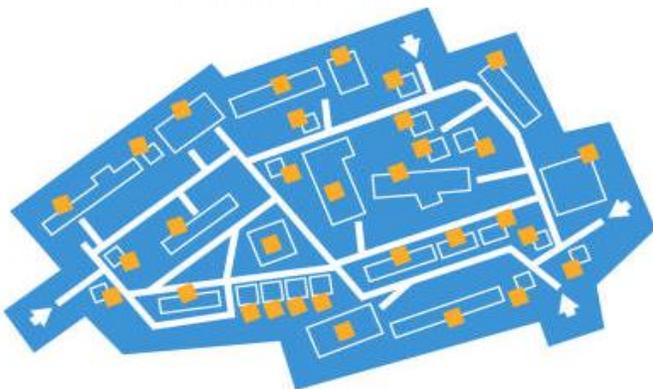
Localización usuarios técnicos con hits USB  
(programadores, administradores de sistemas, etc.)



Cámaras de seguridad?  
Solo apuntan a zonas comunes

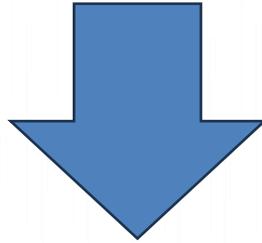


“Triangulación” física



</Caso de estudio – Se estrecha el círculo>

## Forense de los equipos de los usuarios sospechosos



- 1 equipo muestra actividad compatible con el evento
- El usuario buscó cómo borrar trazas de conexión de un USB  
Mala suerte! Encontró la referencia equivocada y no borró la traza!! :S

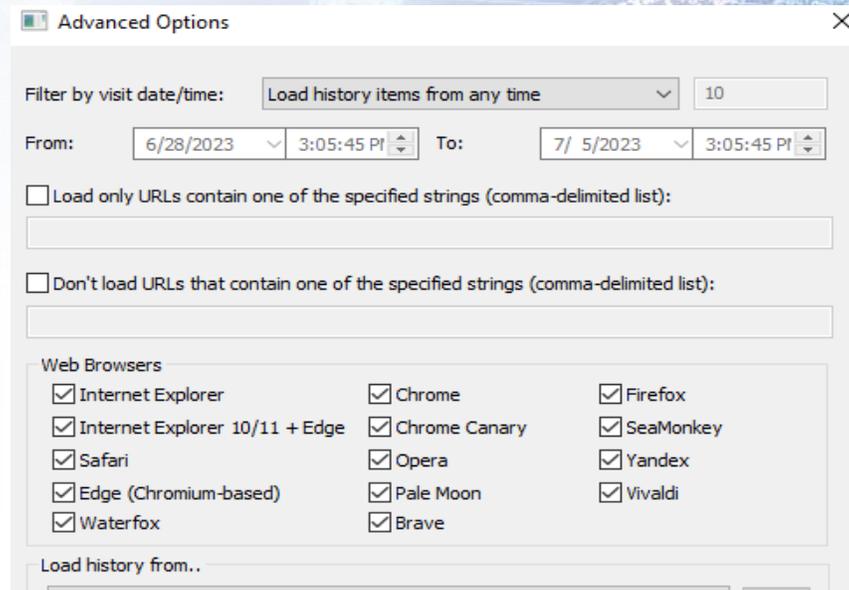
# </Análisis de buscadores web>



WINDOWS REGISTRY HIVES



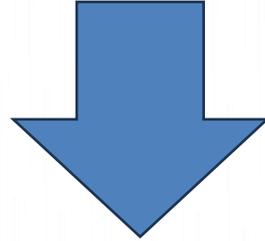
SETUPAPI.DEV.LOG



| URL   | Title  | Visit Time           | Visit Duration |
|---|--|----------------------|----------------|
| https://www.google.com/search?client=firefox-b-1-d&q=google   | google - Buscar con Google                                       | 7/5/2023 2:46:03 PM  |                |
| https://www.google.es/  | Google   | 7/5/2023 2:46:16 PM  |                |
| https://forocoches.com/   | Foros de Foro Coches .com  | 7/5/2023 2:45:35 PM  | 00:00:05.000   |
| https://www.google.com/search?q=forocoches&ei=24GIZM3zNciekdUPpMOPuAg&ved=0ahUKEwiNzfWF5_f...       | forocoches - Buscar con Google                                   | 7/5/2023 2:45:33 PM  | 00:00:01.814   |
| https://www.google.com/search?q=forocoches&ei=24GIZM3zNciekdUPpMOPuAg&ved=0ahUKEwiNzfWF5_f...       | forocoches - Buscar con Google                                   | 7/5/2023 2:45:33 PM  | 00:00:00.537   |
| https://www.mozilla.org/en-US/privacy/firefox/  | Firefox Privacy Notice — Mozilla                                 | 7/22/2022 9:53:41 PM |                |
| https://www.softzone.es/noticias/open-source/yacreader-lector-comics-gratis-open-source/            | Desde que he probado YACReader para leer mis cómics favoritos... | 7/5/2023 2:47:49 PM  |                |
| https://es.wikihow.com/borrar-el-registro-de-conexi%C3%B3n-de-USB-en-un-equipo                      | Cómo borrar el registro de conexión de USB en un equipo          | 7/5/2023 2:46:35 PM  |                |
| https://www.google.es/search?q=como+borrar+trazas+de+haber+conectado+un+usb+en+windows&source...    | como borrar trazas de haber conectado un usb en windows - Bu...  | 7/5/2023 2:46:32 PM  |                |
| https://consent.google.es/m?continue=https://translate.google.es/?hl%3Des&gl=ES&m=0&pc=t&cm=2&hl... | Antes de continuar   | 7/5/2023 2:44:45 PM  | 00:00:02.521   |
| https://consent.google.es/m?continue=https://translate.google.es/?hl%3Des&gl=ES&m=0&pc=t&cm=2&hl... | Antes de continuar   | 7/5/2023 2:45:11 PM  | 00:00:01.453   |

</Caso de estudio - Hemos acabado... no?>

¿Es suficiente?

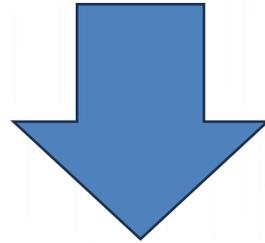


**¡ NO !**

Tenemos al usuario pero no a la persona

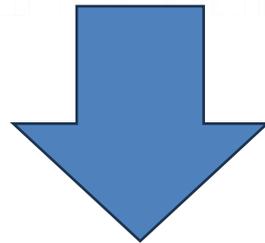
## </Caso de estudio - En busca de la persona >

### Correlación entre usuario y persona

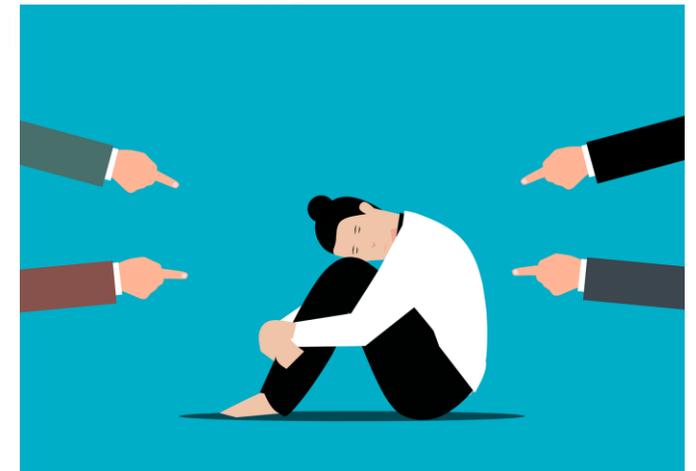


- Patrón de actividad del usuario compatible con su función
- Excusa (no convincente): alguien usó su equipo
- Empleado con comportamiento conflictivo

Es suficiente?



En teoría sí...



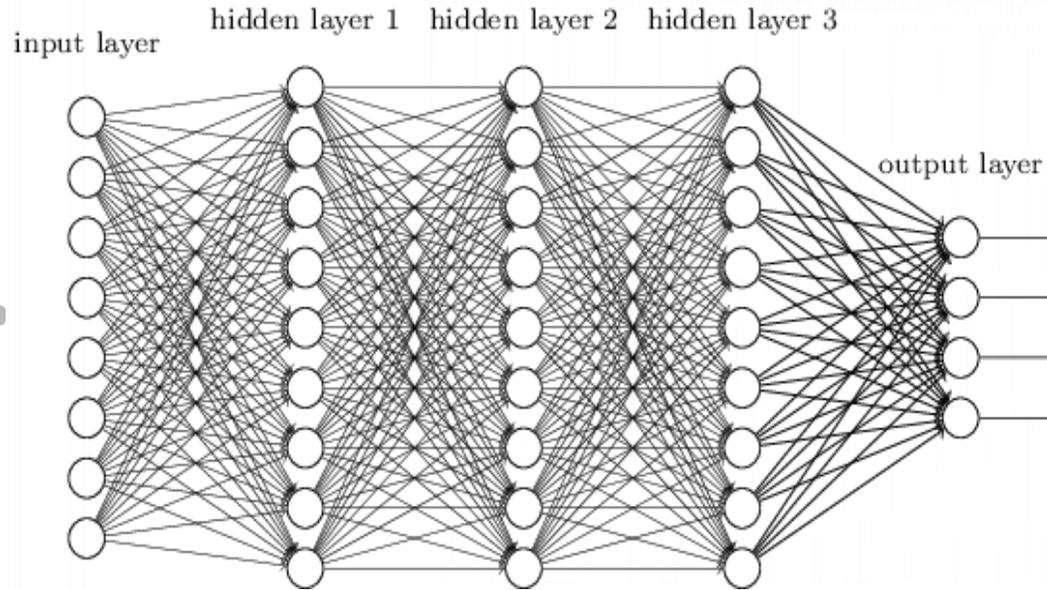
## </ Caso de estudio – Problemática Judicial >

En el mundo real a menudo no!



# </ Identidad y Deep Fakes >

# </Deep Fakes>



*“Los Deep Fakes con propósito criminal son el delito basado en IA con mayor poder de daño (o lucro) de su especie y el más difícil de derrotar”. **Crime Science Journal***

MA Escribe un e-mail para pedir a Francisco que te revise una presentación en la ruta "https://www.drive.google.com/drive/folder/sdhfHFkLkOr" que tienes para una charla en la UMA. Es urgente. ✍

Se conciso.

 Asunto: Revisión urgente de presentación para charla en la UMA 📄

Estimado Francisco,

Espero que este correo electrónico te encuentre bien. Te escribo para solicitarte un favor urgente. Tengo una presentación importante para una charla en la Universidad de Málaga (UMA) y necesitaría que revises el contenido.

La presentación se encuentra en la siguiente ruta de Google Drive:

<https://www.drive.google.com/drive/folder/sdhfHFkLkOr>. Sería de gran ayuda si pudieras acceder a ella lo antes posible y proporcionarme tus comentarios y sugerencias para mejorarlo.

Dado que la charla está programada para un futuro cercano, agradecería mucho si pudieras realizar la revisión en un plazo de 24 horas. Tu experiencia y conocimiento son invaluable para mí, y confío en tu juicio para ayudarme a pulir este material y asegurar una presentación efectiva.

Quedo a la espera de tu respuesta y agradezco de antemano tu amabilidad y disposición para ayudarme. Si tienes alguna pregunta o necesitas más información, no dudes en hacérmelo saber.

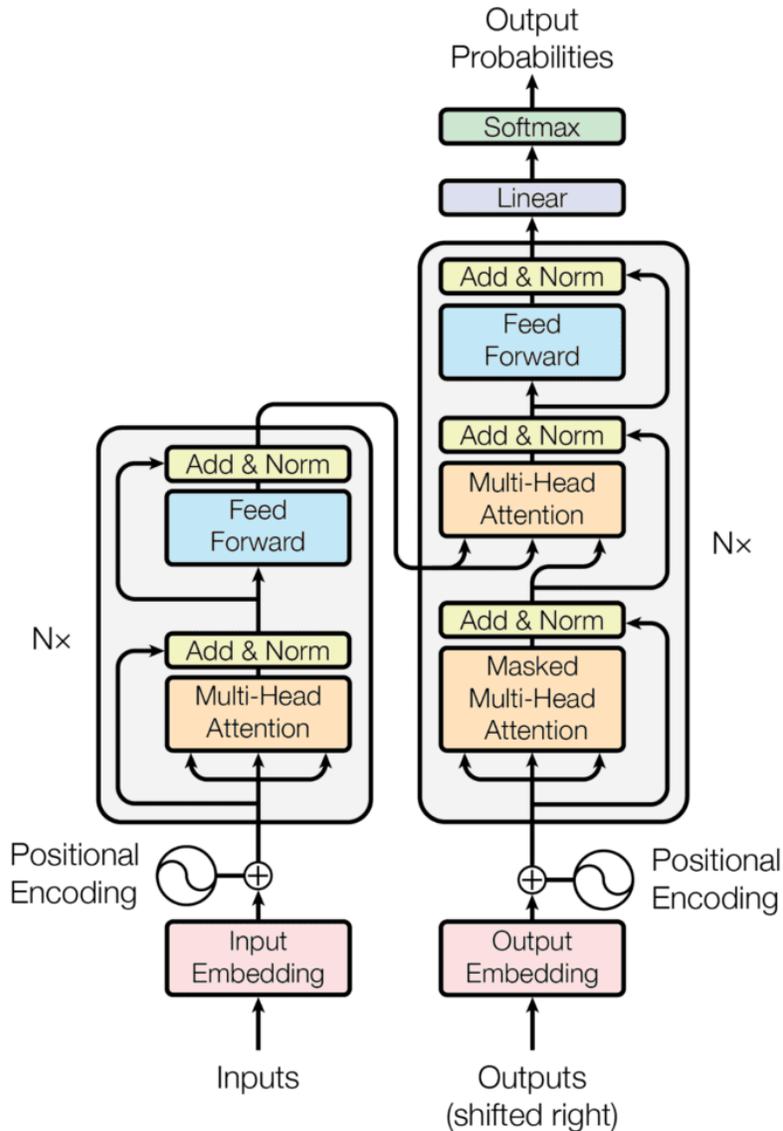
¡Muchas gracias!

Saludos cordiales,

 Regenerate response



# </Transformers>

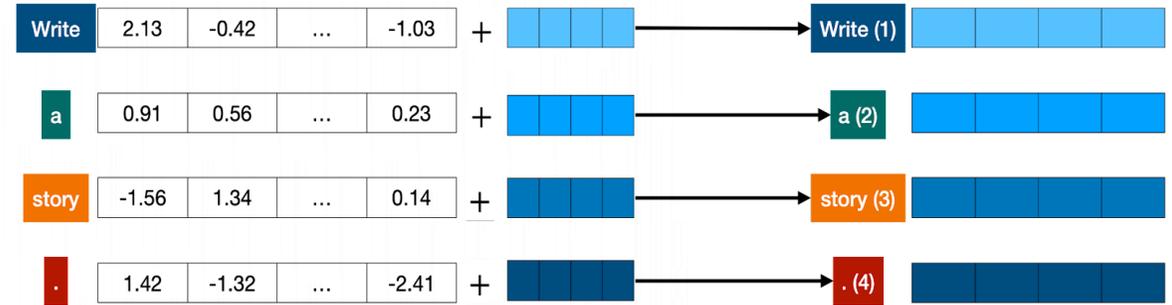


TOKENIZATION

POSITIONAL ENCODER

ATTENTION MECHANISM

Write a story. → Write A story .



The **door** of the **jaguar** were opened.  
The **jaguar** made a **howling** noise.

<https://towardsdatascience.com/transformers-141e32e69591>

## </Creación de Deep Fakes>



```
File Edit Selection View Go Run Terminal Help
DeepFakes.ipynb X
+ Code + Markdown | ▶ Run All ≡ Clear All Outputs | ≡ Outline ...
Select Kernel

image = imageio.imread('/home/user/src/UMA_summer/first-order-model/demo/img_1.png')
video = imageio.mimread('/home/user/src/UMA_summer/first-order-model/demo/vid_1.mp4')

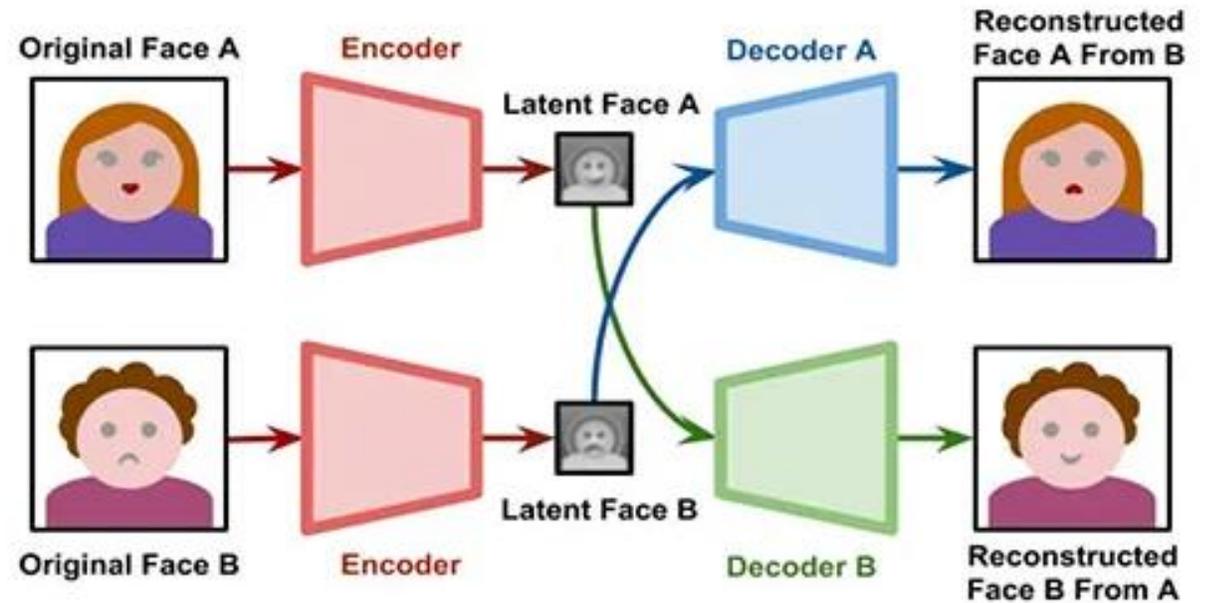
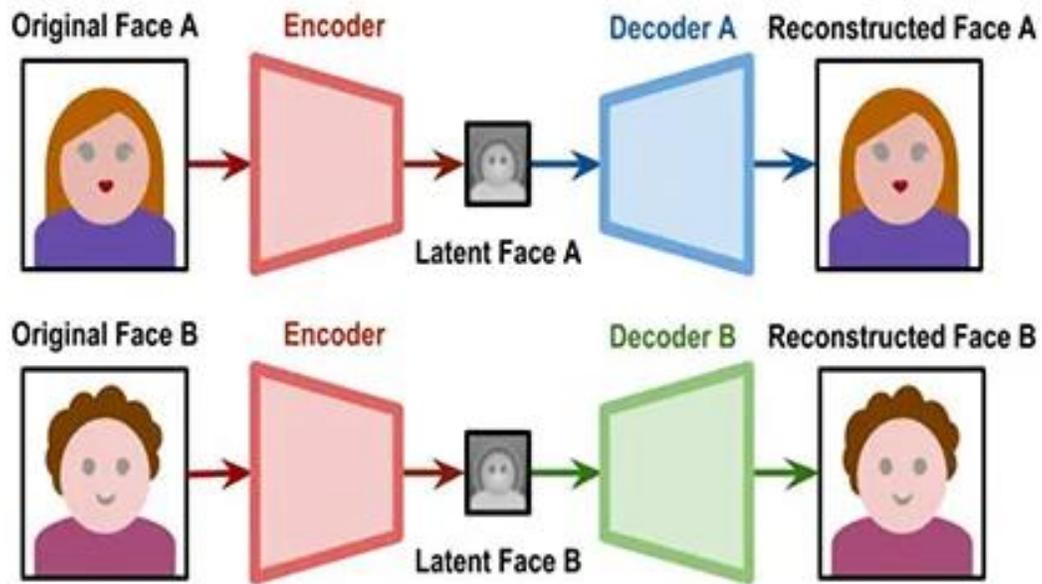
# Create the model
generator, detector = load_checkpoints(config_path='config/vox-256.yaml',
                                     checkpoint_path='/home/user/src/UMA_summer/first-order-model/vox-cpk.pth.tar', cpu=True)

# DeepFake generator
predictions = make_animation(image, video, generator, detector, relative=True, cpu=True)

# Save results
imageio.mimsave('../output.mp4', [img_as_ubyte(frame) for frame in predictions])

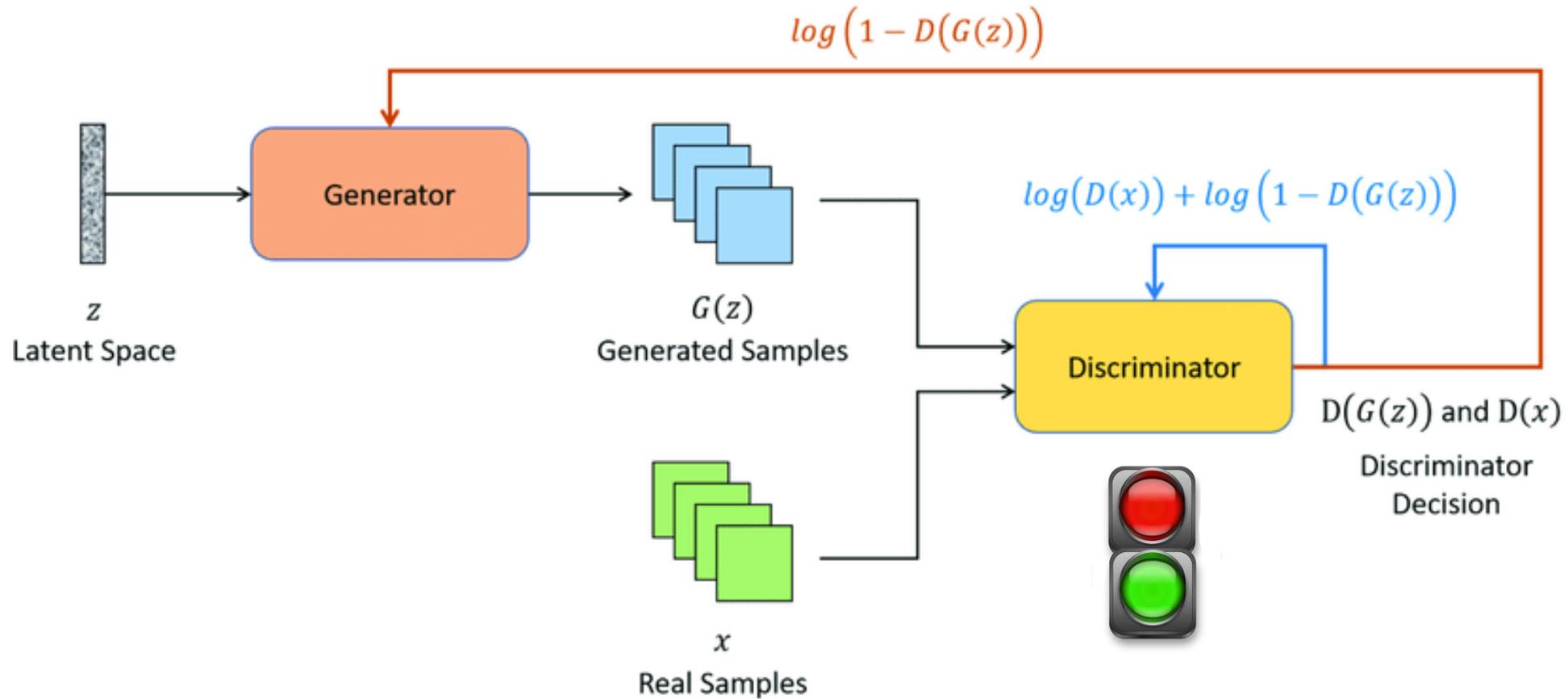
[17] Python
```

<https://github.com/AliaksandrSiarohin/first-order-model>



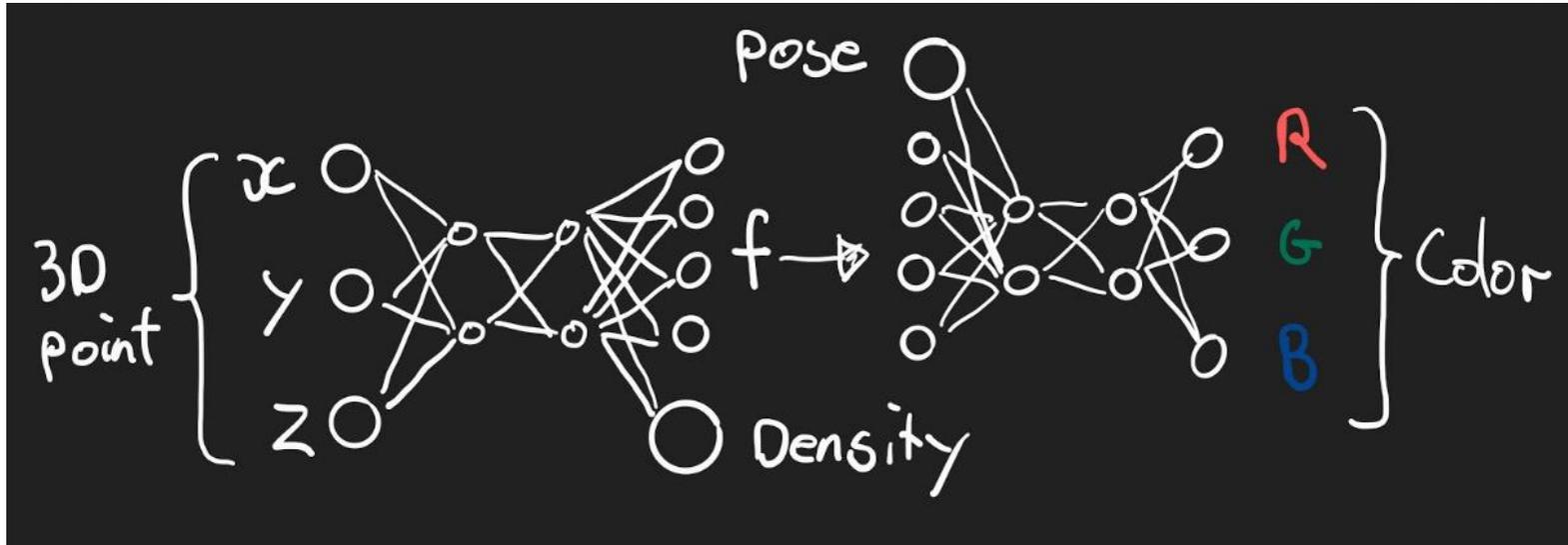
<https://www.oreilly.com/library/view/generating-a-new/9781484270929/>

# </Generative Adversarial Network (GAN)>



<https://github.com/enochkan/awesome-gans-and-deepfakes>

# </Neural Radiance Fields (NeRF)>

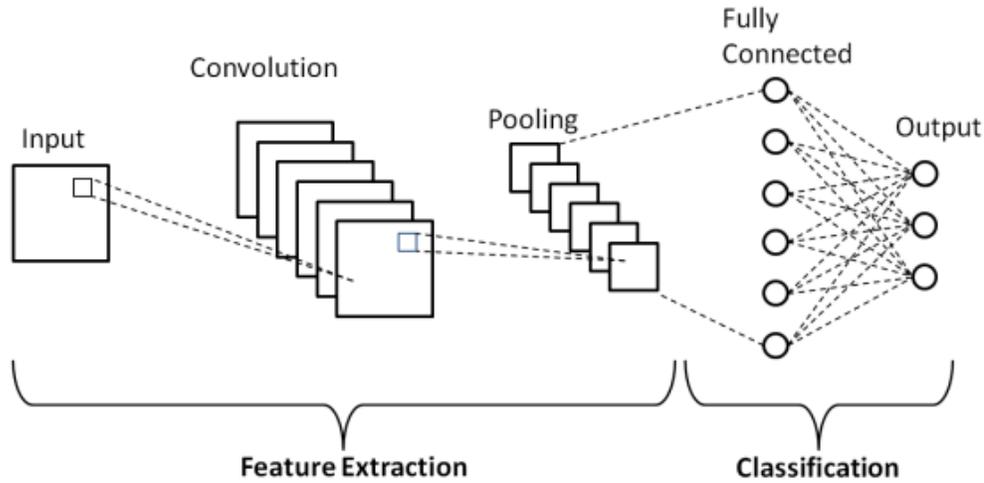


MULTILAYER  
PERCEPTRON



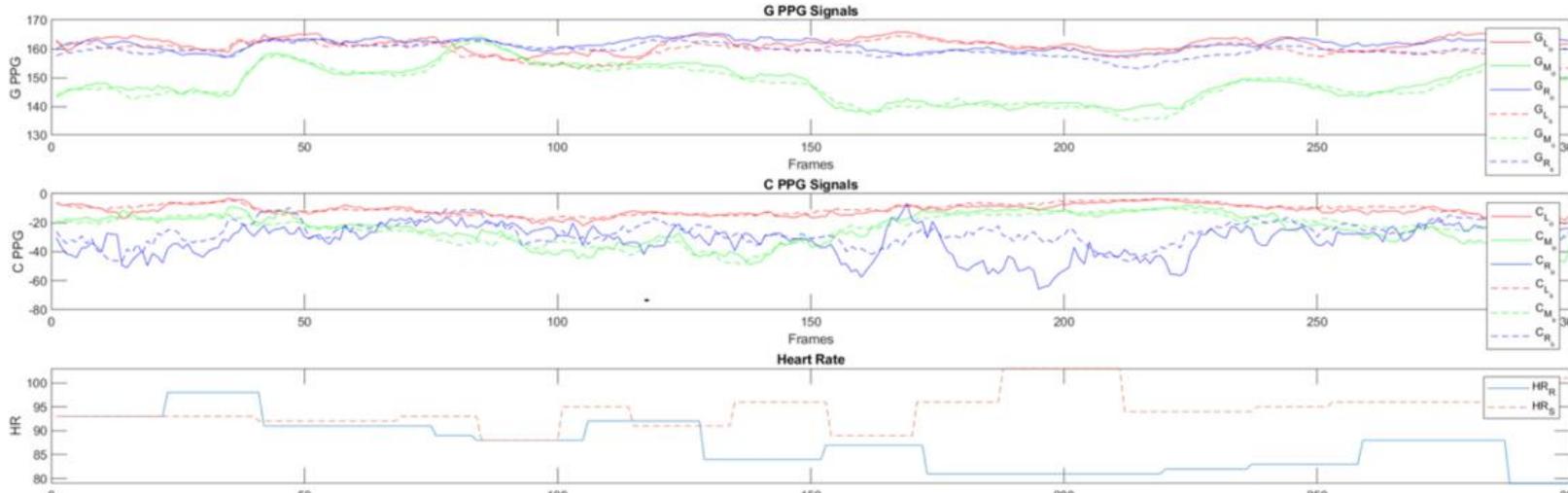
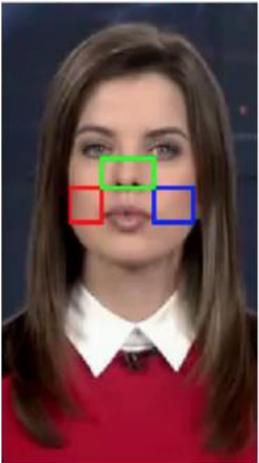
<https://stfwn.com/articles/neural-radiance-fields/>

# </Deep Fakes Forensics>

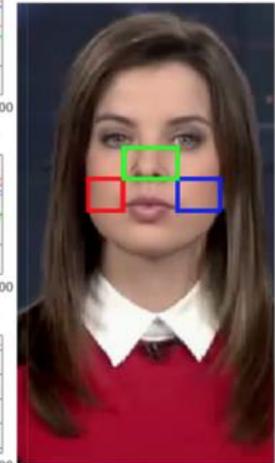


## Convolutional Neural Networks

Original Image

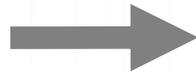
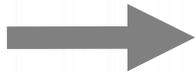


Synthetic Image

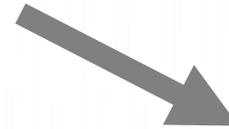


<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9141516>

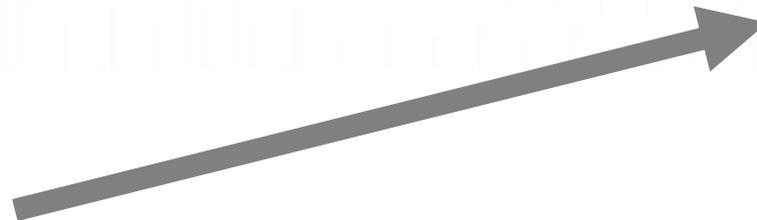
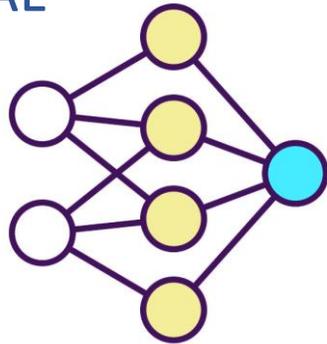
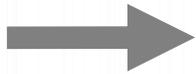
HUMANOS



PENSAMIENTO  
SIMBÓLICO

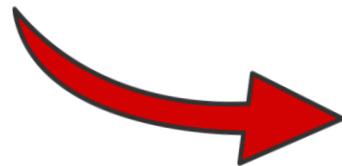


INTELIGENCIA ARTIFICIAL



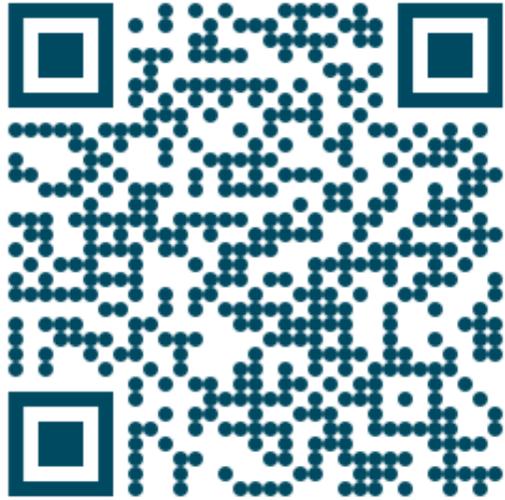
TOMA DE  
DECISIONES

# </Problemática Judicial>



## </Conclusiones>

- <c1> **Diferenciar entre identidad y persona </c1>**
- <c2> ***Digital Forensic* clave para determinar identidad en fraudes online </c2>**
- <c3> **Problemática en el uso de evidencias digitales en procesos legales <c/3>**
- <c4> **Deep Fakes, una nueva y poderosa arma para suplantación de identidad </c4>**
- <c5> **Las leyes actuales no están adaptadas a las Deep Fakes </c5>**
- <c6> **Problema ético en el uso de la IA en la toma de decisiones </c6>**



# MUCHAS GRACIAS

[www.one-esecurity.com/events\\_training/2023/umacv23.html](http://www.one-esecurity.com/events_training/2023/umacv23.html)



## Jess Garcia

[jess.garcia@one-esecurity.com](mailto:jess.garcia@one-esecurity.com)

[@j3ssgarcia](https://twitter.com/j3ssgarcia)

**Research Team:**

**Mario Perez**

### DS4N6



[ds4n6.io](http://ds4n6.io)



[@ds4n6\\_io](https://twitter.com/ds4n6_io)



[DS4N6](https://www.youtube.com/DS4N6)



[one-esecurity.com](http://one-esecurity.com)



[@One\\_eSecurity](https://twitter.com/One_eSecurity)



[one-esecurity](https://www.linkedin.com/company/one-esecurity)



**Making the world safer since 2007**

**San Francisco · Miami · Mexico City · São Paulo · Madrid · London · Singapore · Santiago de Chile · Bogotá**

[www.one-esecurity.com](http://www.one-esecurity.com) | [ds4n6.io](http://ds4n6.io)