Experiencias propias en la contribución a proyectos de software libre: Volatility

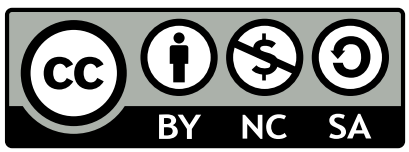
Ricardo J. Rodríguez

Universidad Zaragoza

Dept. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza

13 de mayo, 2023

esLibre
Zaragoza, España



$whoami

- **Profesor Titular de Universidad**
- **Líneas de investigación**:
  - Análisis de software
  - Forense digital
  - Seguridad ofensiva
  - Análisis de seguridad y supervivencia con modelos formales

Universidad Zaragoza

$whoami

- **Profesor Titular de Universidad**
- **Líneas de investigación**:
  - Análisis de software
  - Forense digital
  - Seguridad ofensiva
  - Análisis de seguridad y supervivencia con modelos formales
- **Equipo de investigación** – *¡hacemos cosas chulas!* 🙂
  - `https://reversea.me`
  - `https://twitter.com/reverseame/`
  - `https://t.me/reverseame`

Dr. Javier Carrillo

Post-doc

Daniel Uroz

Razvan Raducu

Estudiantes PhD

Daniel Huici

Miguel Moniente

Estudiantes TFM

Universidad Zaragoza 1542

Agenda

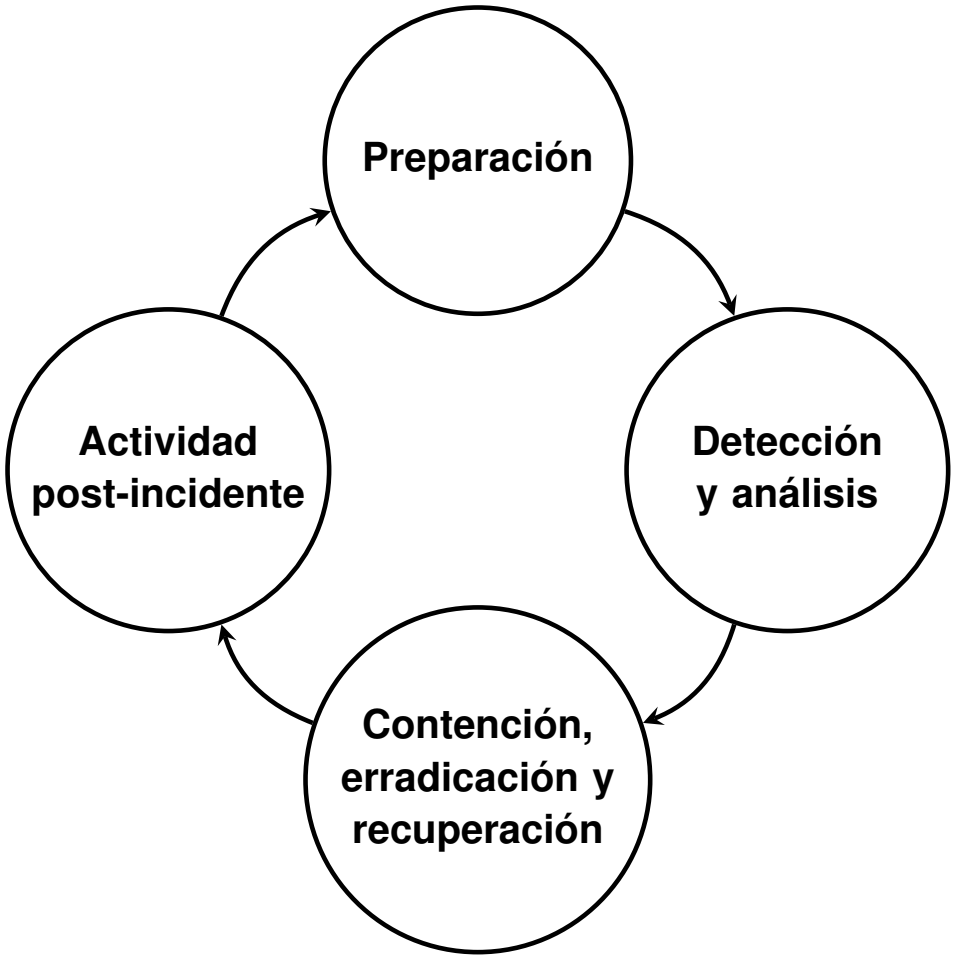
Universidad Zaragoza

Agenda

Universidad Zaragoza

Introducción

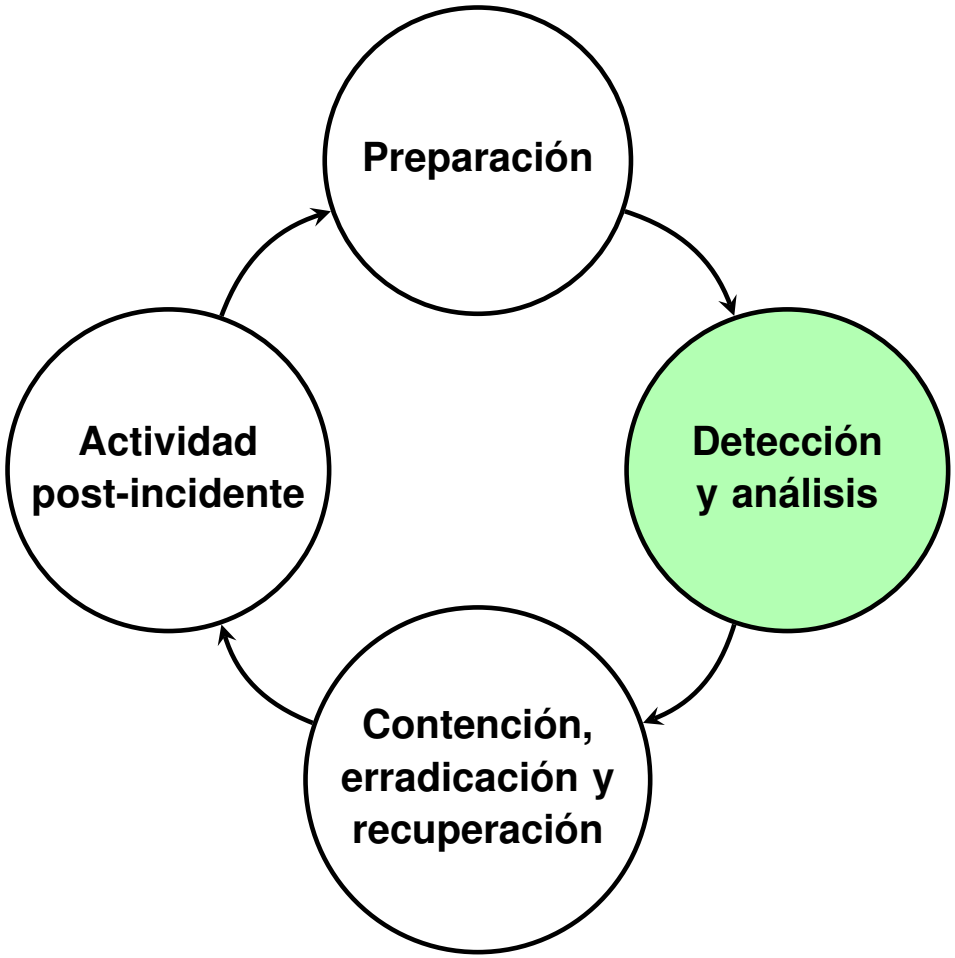
Un poco de recapitulación...



Respuesta a incidentes definida por el NIST

Introducción

Un poco de recapitulación...



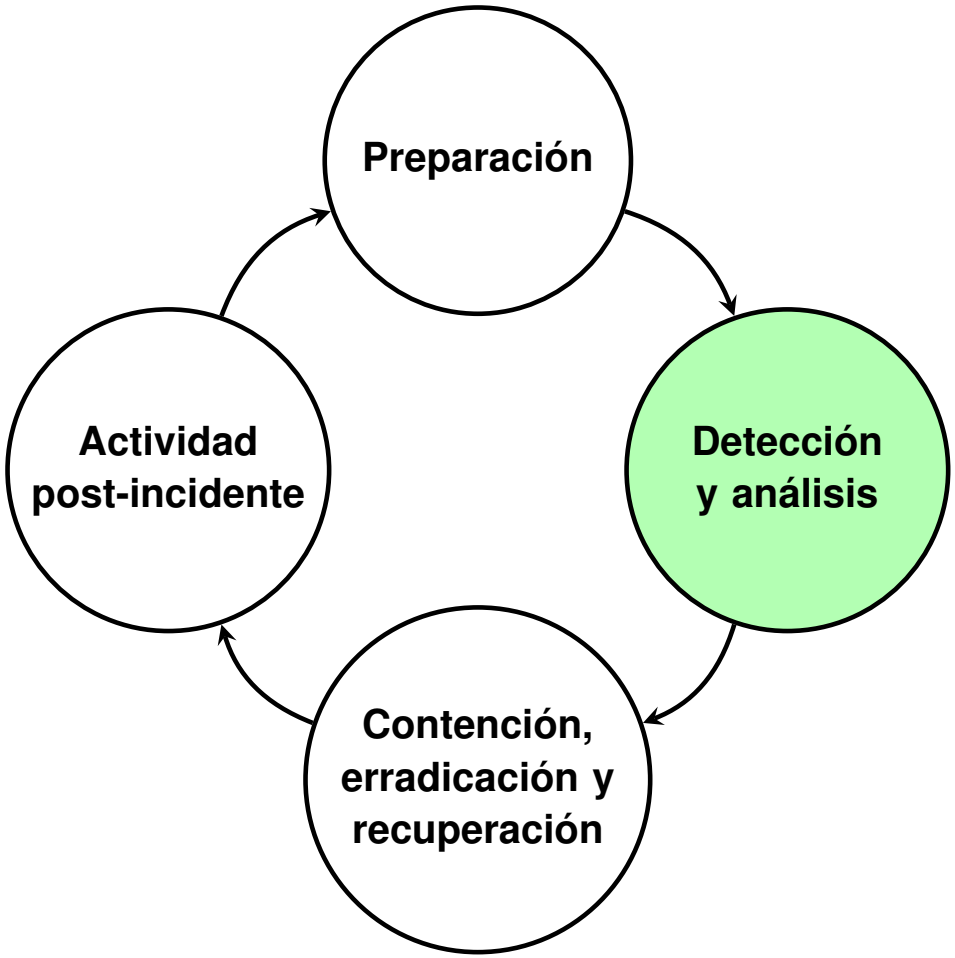
Respuesta a incidentes definida por el NIST

- **Análisis forense de red**
- **Análisis forense de ordenadores**
  - Disco + **memoria**

Universidad Zaragoza

Introducción

Un poco de recapitulación...



Respuesta a incidentes definida por el NIST

- **Análisis forense de red**
- **Análisis forense de ordenadores**
  - Disco + **memoria**

Disco vs. memoria

- Algunas veces, **el acceso a dispositivos físicos es difícil**
- **Límites actuales de capacidad de almacenamiento vs. capacidad de la memoria**
  - Terabytes versus gibibytes
  - **Facilita el triaje inicial**
- Algunos datos sólo residen en memoria

Universidad Zaragoza

Introducción

Análisis forense de memoria

Volcado de memoria

- **Lleno de datos** para analizar
- **Cada elemento que se puede analizar se llama *artefacto* de memoria**
  - Recuperados vía estructuras internas del SO o búsquedas de patrones
- "Foto" de los procesos en ejecución, usuarios activos, archivos abiertos, o conexiones de red abiertas – **todo lo que estaba en ejecución en el momento de captura**
- Puede contener también **recursos liberados recientemente**
  - Normalmente, la memoria no se "pone a cero" cuando se libera

Universidad Zaragoza

Agenda

Universidad Zaragoza
1542

Volatility

- Herramienta **estándar de facto** de análisis de memoria forense
  - Versión 2 vs. versión 3 ⇒ Python2 vs. Python3
- **Útil para examinar y extraer información de la memoria volátil**
- Compatible con amplia gama de sistemas operativos
- **Perfiles**: información sobre estructura de la memoria del sistema operativo

`https://github.com/volatilityfoundation/volatility3`

Universidad Zaragoza
1542

Agenda

Universidad Zaragoza

Nuestra primera experiencia con Volatility

- **Necesidad de investigación en 2016**, trabajando con Miguel Martín:
  - **Hashes criptográficos vs. hashes de similitud aproximada** (e..g, MD5 vs. ssdeep)
  - $m \in \{0, 1\}$ ($m \in \mathbb{Z}$) vs. $m \in [0, 1]$ ($m \in \mathbb{R}$)

Universidad Zaragoza
1542

Nuestra primera experiencia con Volatility

- **Necesidad de investigación en 2016**, trabajando con Miguel Martín:
  - **Hashes criptográficos vs. hashes de similitud aproximada** (e..g, MD5 vs. ssdeep)
  - $m \in \{0, 1\}$ ($m \in \mathbb{Z}$) vs. $m \in [0, 1]$ ($m \in \mathbb{R}$)
  - **Aplicación a procesos extraídos de memoria**
  - Más información: doi: 10.1016/j.fsidi.2021.301120

Universidad Zaragoza
1542

Nuestra primera experiencia con Volatility

- **Necesidad de investigación en 2016**, trabajando con Miguel Martín:
  - **Hashes criptográficos vs. hashes de similitud aproximada** (e..g, MD5 vs. ssdeep)
  - $m \in \{0, 1\}$ ($m \in \mathbb{Z}$) vs. $m \in [0, 1]$ ($m \in \mathbb{R}$)
  - **Aplicación a procesos extraídos de memoria**
  - Más información: doi: 10.1016/j.fsidi.2021.301120
- Plugin `ProcessFuzzyHash`, desarrollado por Iñaki Abadía Osta (TFG GII, curso 2016/2017; actualmente *Senior Engineer* en Arm)
  - Falta de documentación sobre cómo desarrollar plugins
  - `https://webdiis.unizar.es/~ricardo/files/TFGs/FuzzyHashingProcesos.pdf`
  - `https://github.com/reverseame/processfuzzyhash`

Universidad Zaragoza

Nuestra primera experiencia con Volatility

- Participación con `ProcessFuzzyHash` en *2017 Volatility Plugin Contest*
  - `https://volatility-labs.blogspot.com/2017/11/results-from-5th-annual-2017-volatility.html`

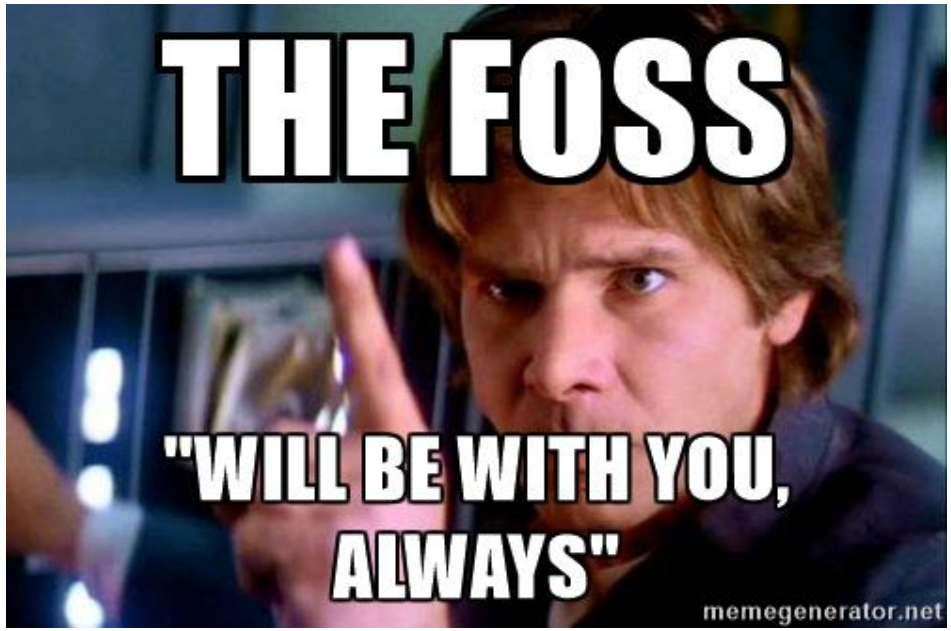
Universidad Zaragoza

Nuestra primera experiencia con Volatility

- Participación con `ProcessFuzzyHash` en *2017 Volatility Plugin Contest*
  - `https://volatility-labs.blogspot.com/2017/11/results-from-5th-annual-2017-volatility.html`
  - No ganamos 😕
  - *Big kudos to Xabier!*
- **Resultado: plugin añadido a repositorio oficial**
  - `https://github.com/volatilityfoundation/community/tree/master/ProcessFuzzyHash`

Universidad Zaragoza

Nuestra primera experiencia con Volatility



- Manera diferente de participar en comunidad FOSS: concurso anual
  - Extensión independiente de las capacidades de la herramienta “madre”
  - Incorporación al repositorio. **Contras**: mantenimiento
  - Detección de errores y posibles soluciones a la herramienta (durante el uso)

Universidad Zaragoza
1542

Agenda

Universidad Zaragoza
1542

Nuestra experiencia actual con Volatility

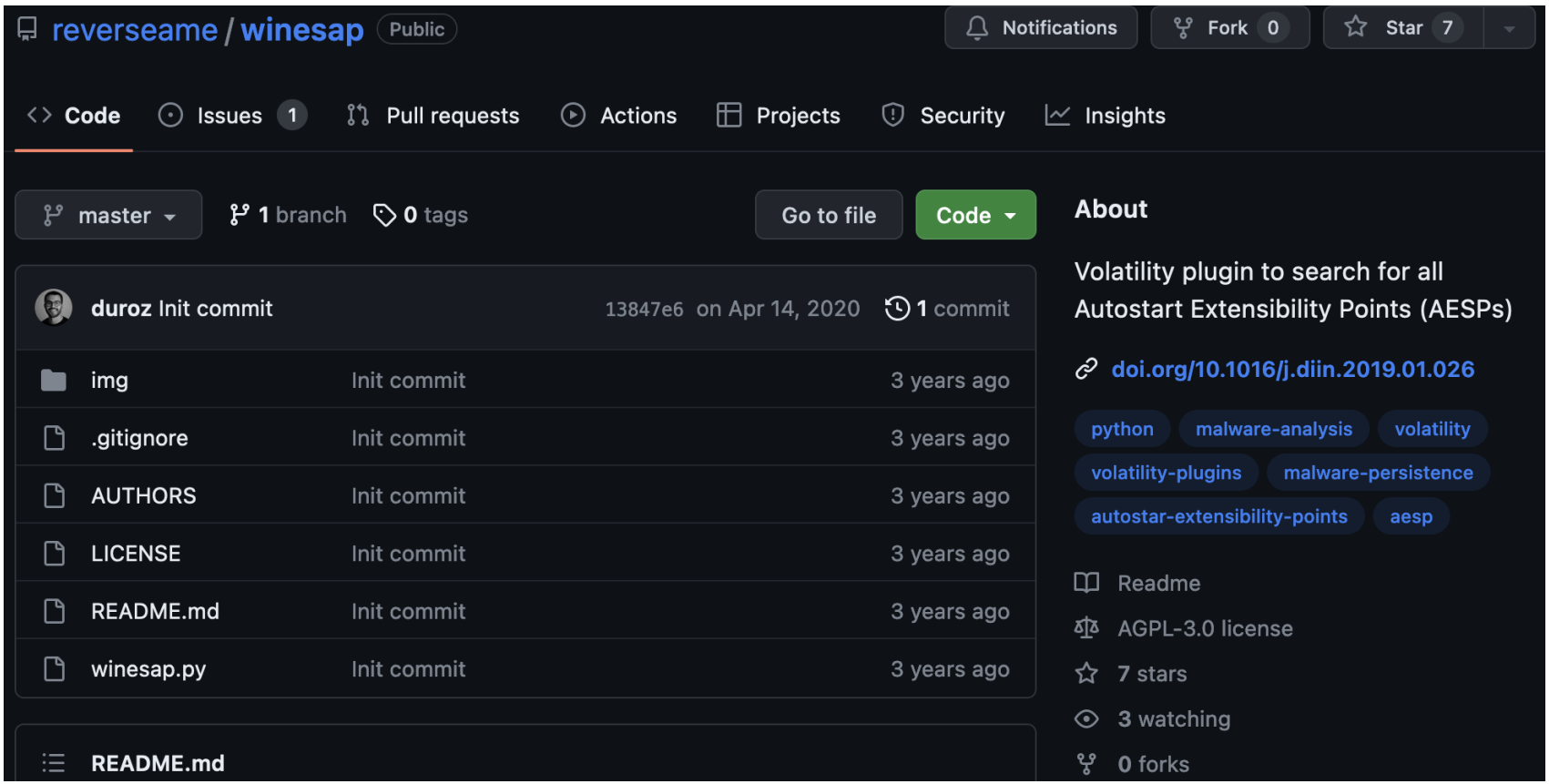
- Actualmente, ya no participamos en los concursos... (mucha burocracia)
- Pero **seguimos liberando todo bajo GNU/GPLv3**
  - *Parte de nuestro compromiso ético con la ciencia abierta y con proyectos FOSS*

Créditos: https://www.flickr.com/photos/opensourceway/4812651268

Universidad Zaragoza

Nuestra experiencia actual con Volatility

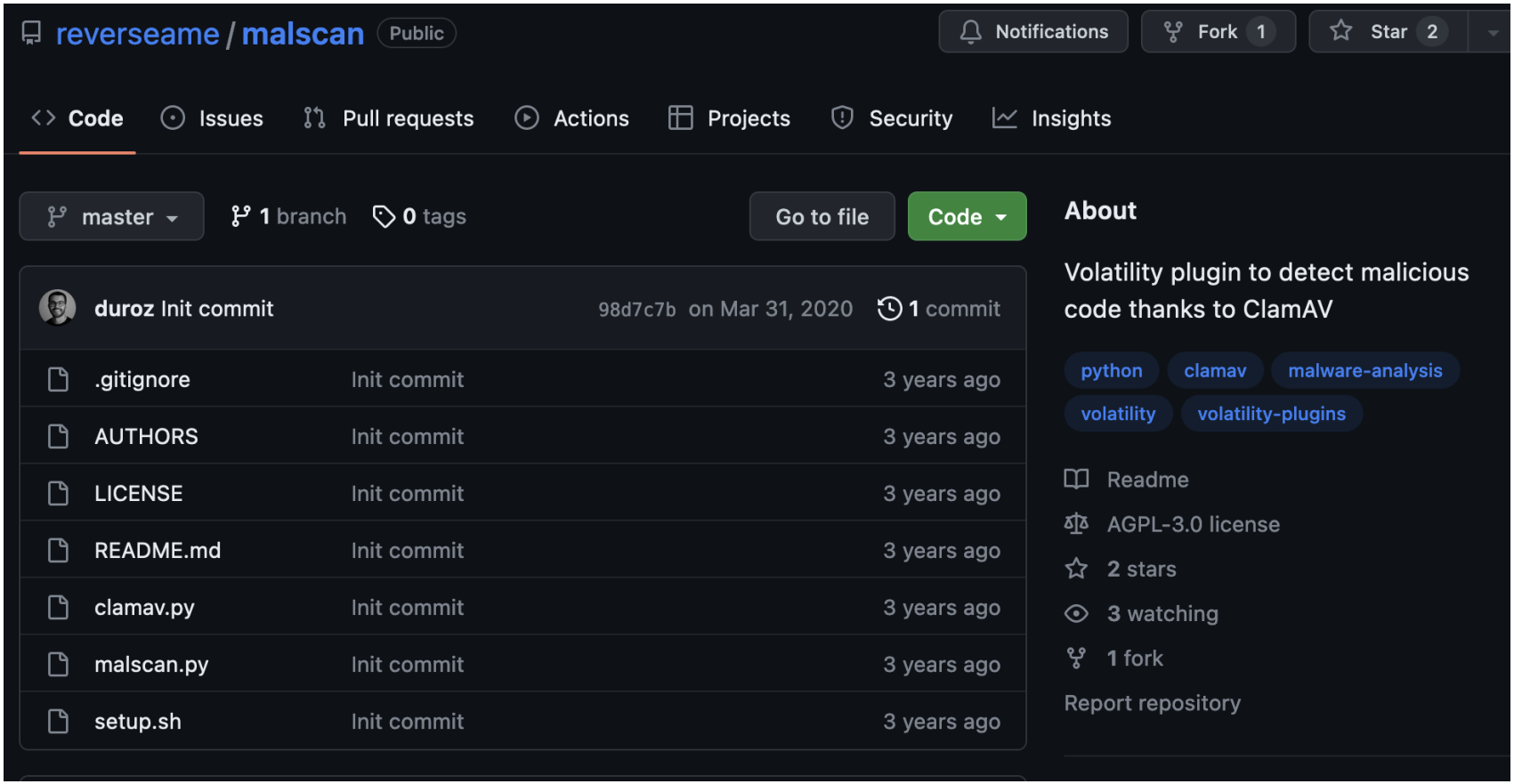
Herramienta `winesap`



`https://github.com/reverseame/winesap`

Nuestra experiencia actual con Volatility

Herramienta `malscan`

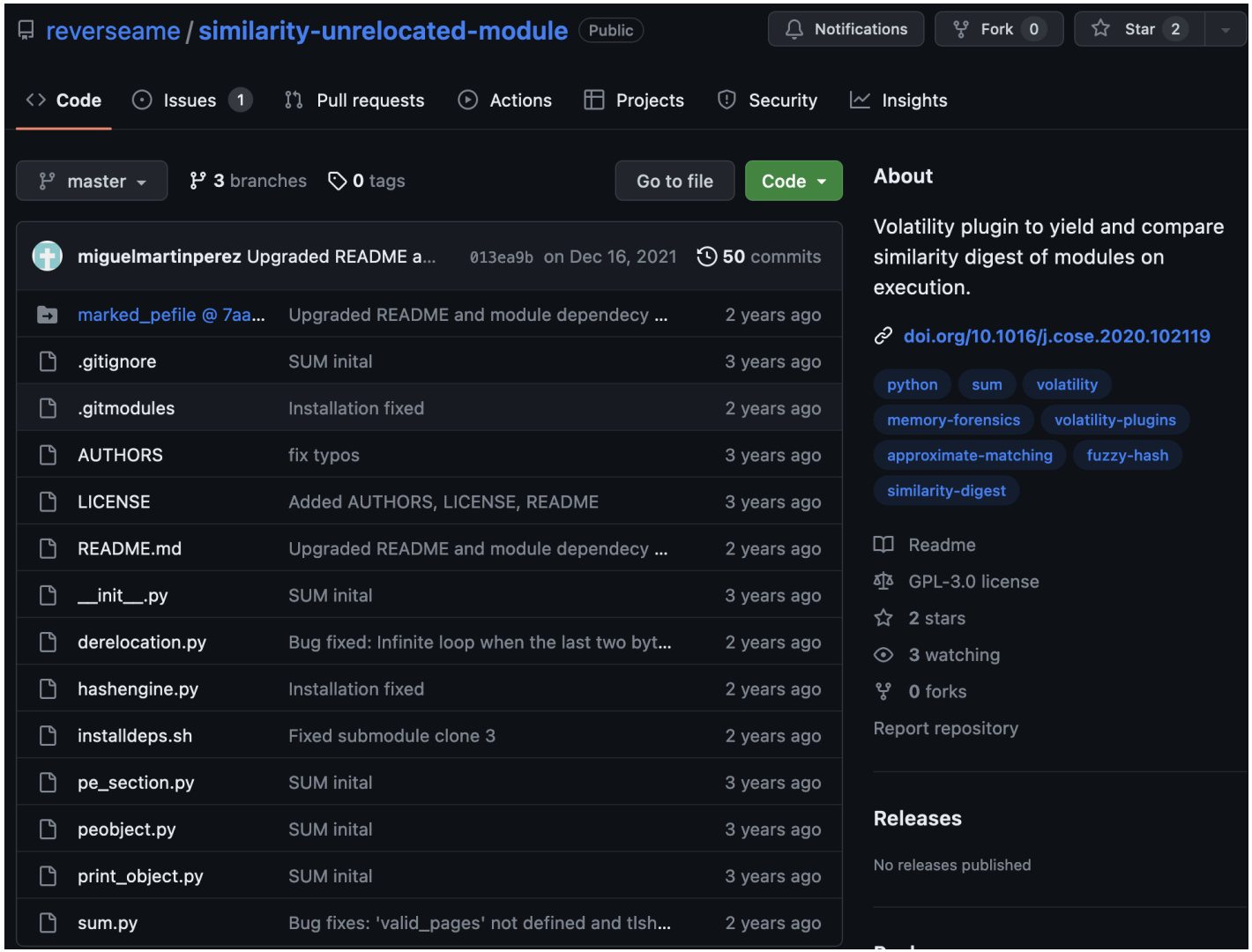


`https://github.com/reverseame/malscan`

Universidad Zaragoza

Nuestra experiencia actual con Volatility

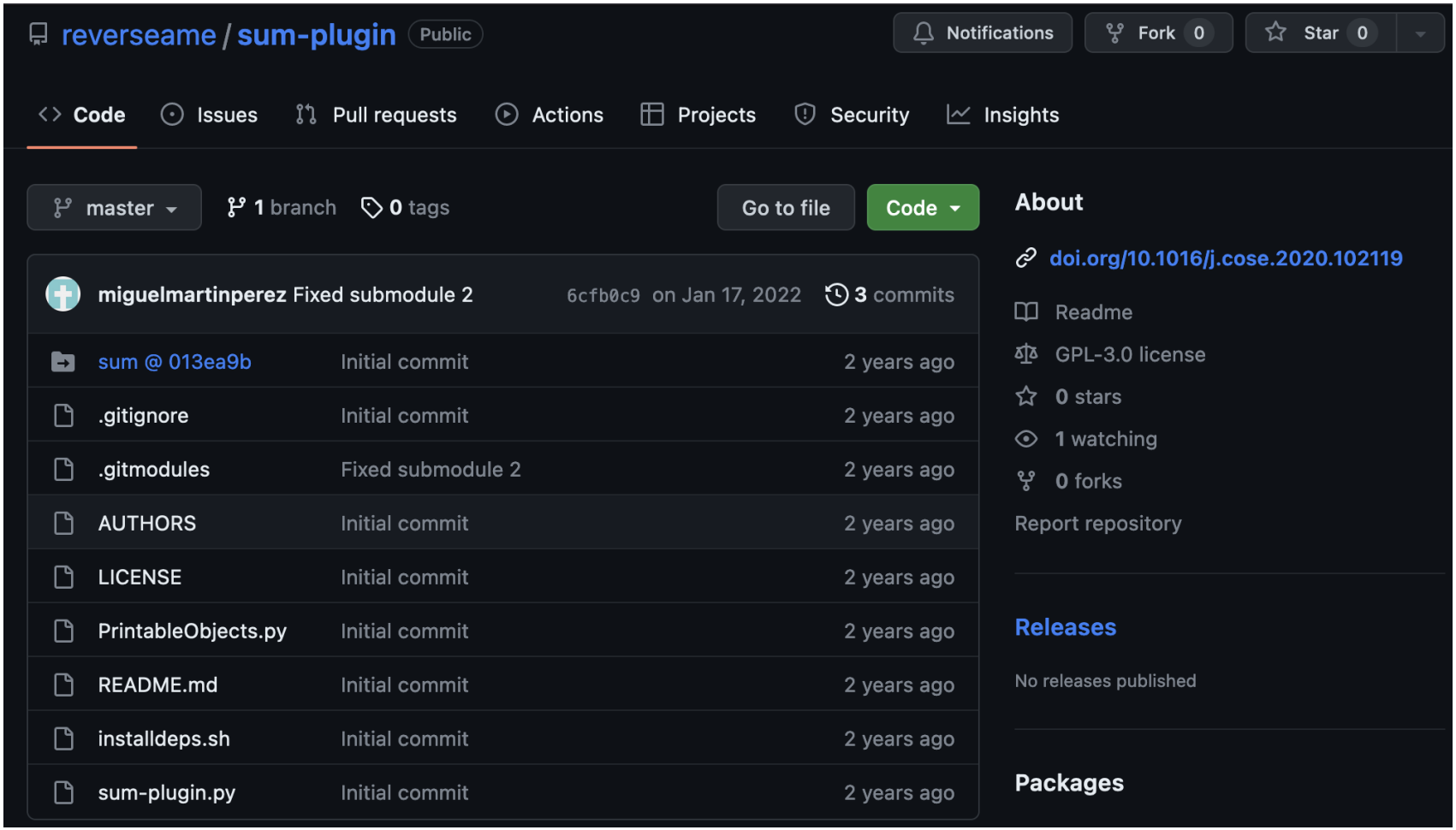
Herramienta `similarity-unrelocated-module`



`https://github.com/reverseame/similarity-unrelocated-module`

Nuestra experiencia actual con Volatility

Herramienta `sum-plugin`

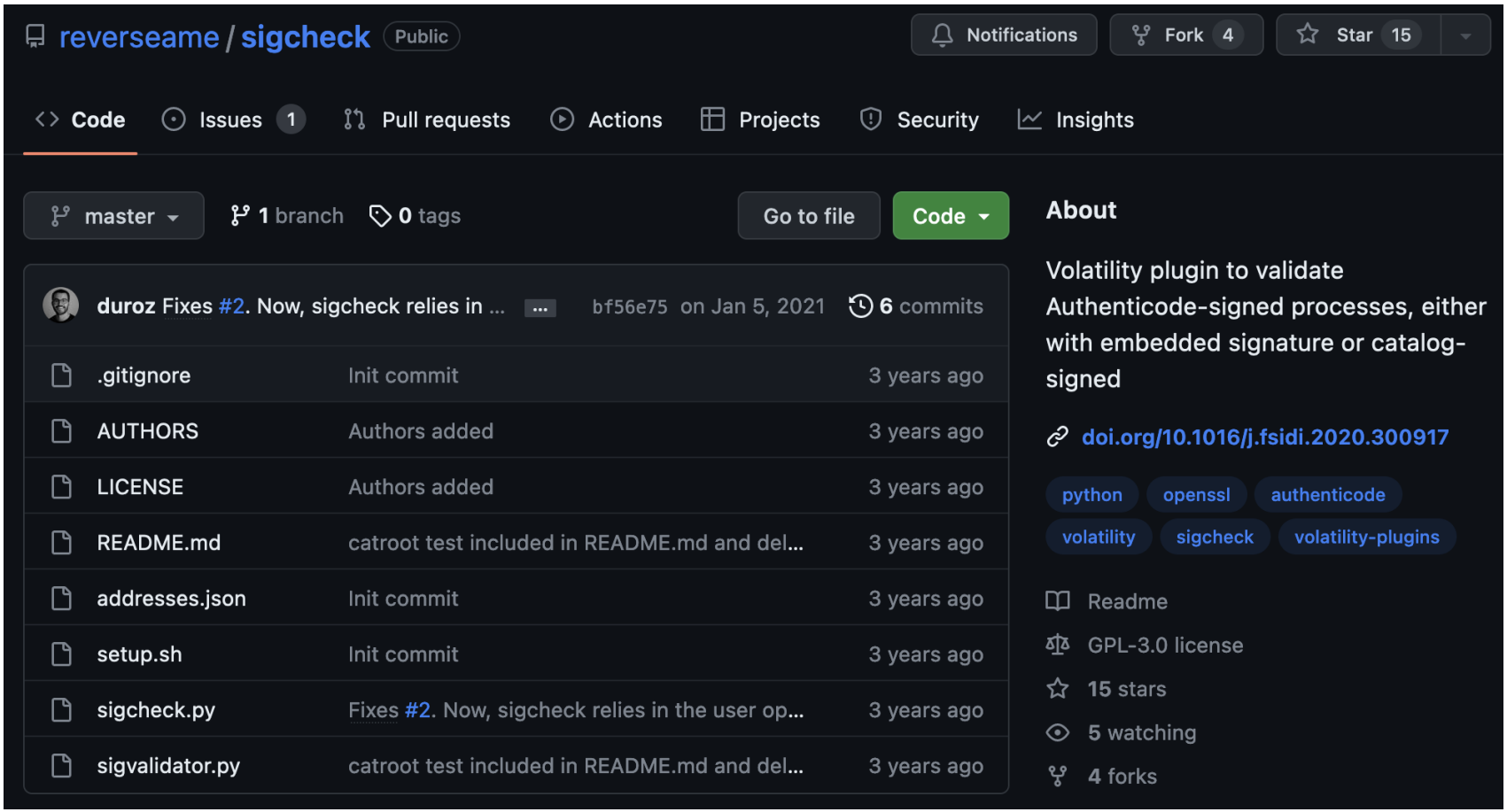


`https://github.com/reverseame/sum-plugin`

Universidad Zaragoza

Nuestra experiencia actual con Volatility

Herramienta `sigcheck`

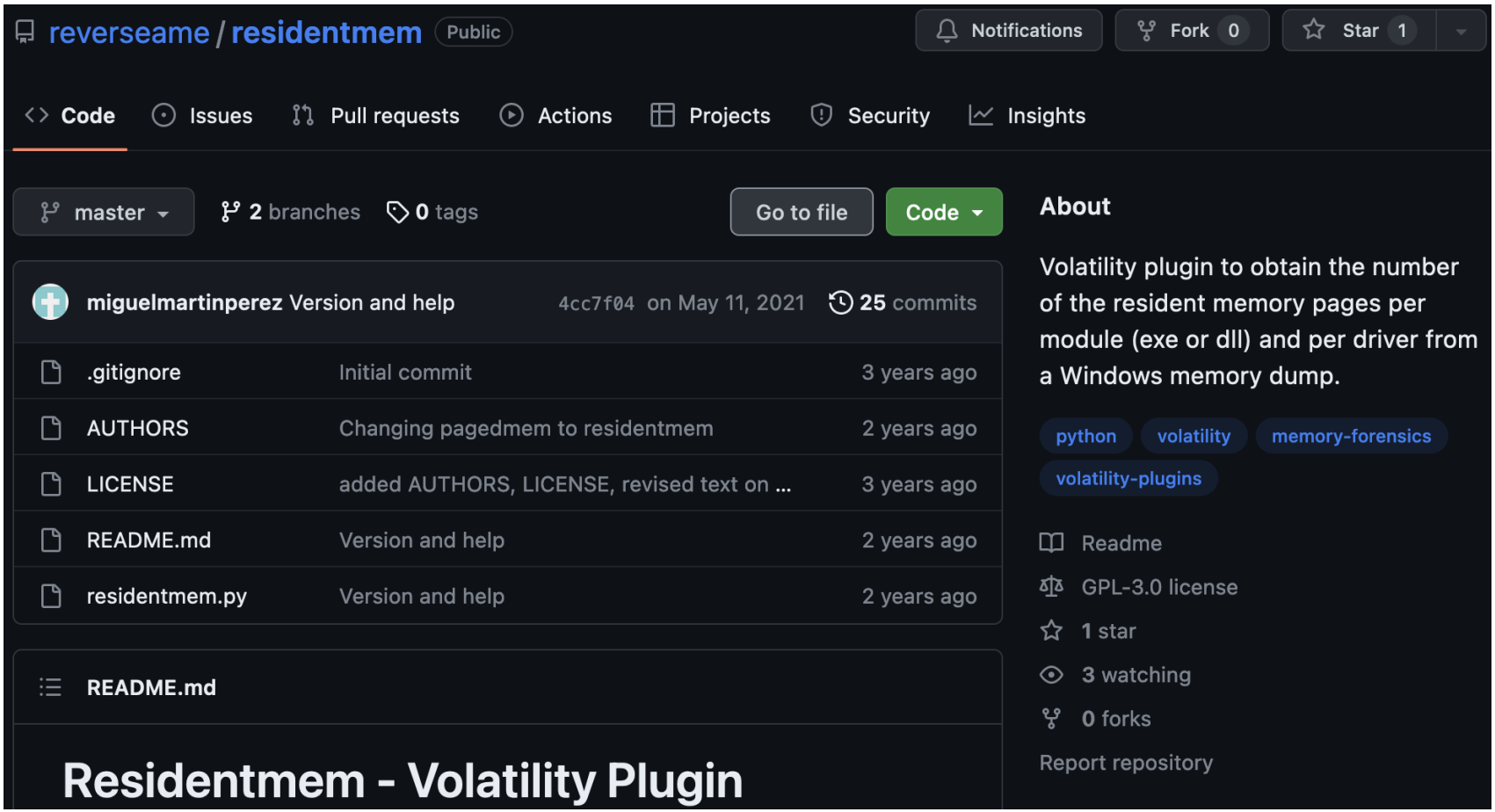


`https://github.com/reverseame/sigcheck`

Universidad Zaragoza

Nuestra experiencia actual con Volatility

Herramienta `residentmem`

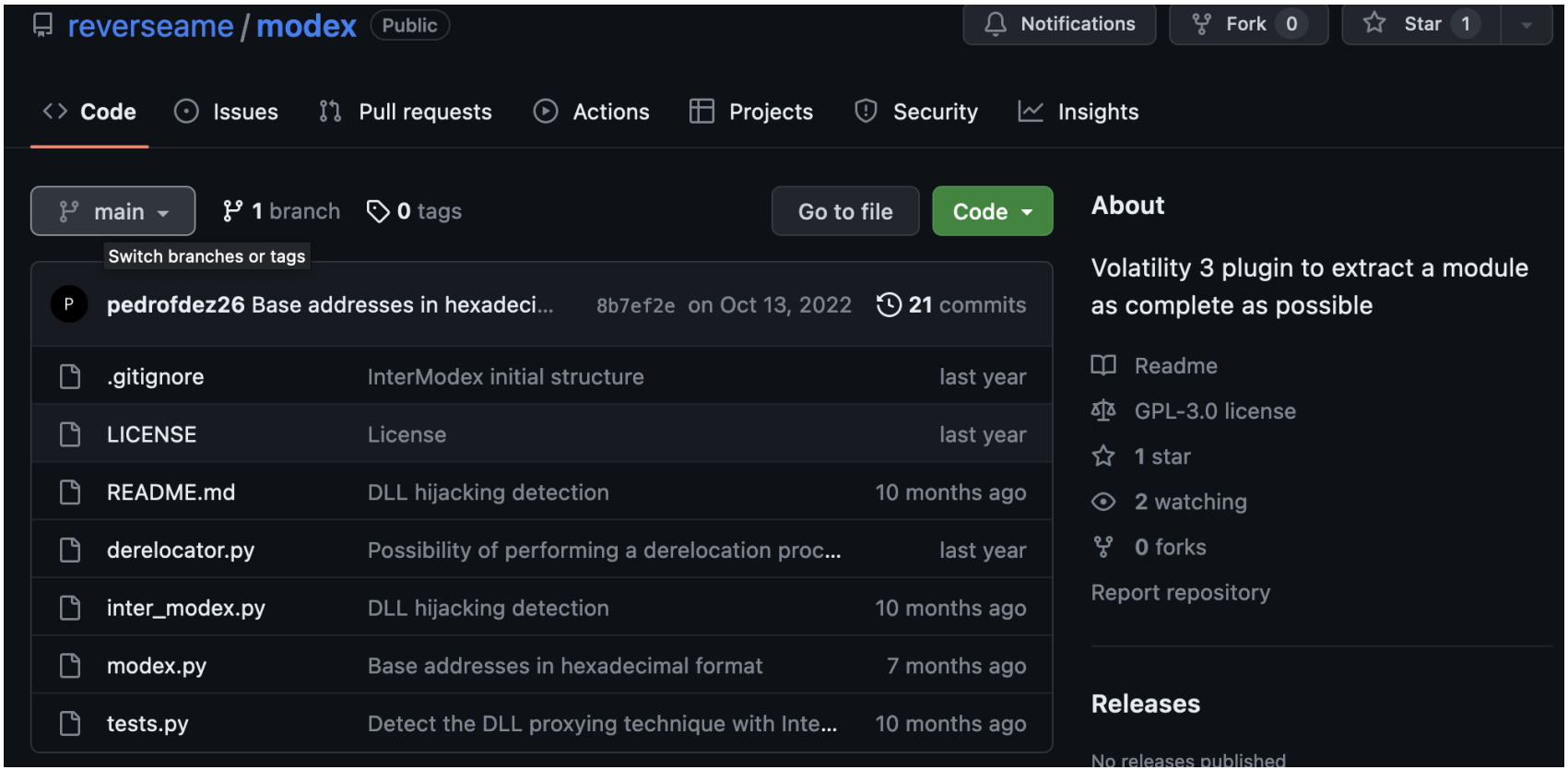


`https://github.com/reverseame/residentmem`

Universidad Zaragoza

Nuestra experiencia actual con Volatility

Herramienta `modex`



`https://github.com/reverseame/modex`

Universidad Zaragoza

Agenda

Universidad Zaragoza

Conclusiones

- **+6 plugins desarrollados para Volatility**
  - Buena acogida de la comunidad (científica, sobre todo)
  - Contacto con Volexity (`https://www.volexity.com/`)

Universidad Zaragoza

Conclusiones

- **+6 plugins desarrollados para Volatility**
  - Buena acogida de la comunidad (científica, sobre todo)
  - Contacto con Volexity (`https://www.volexity.com/`)
- **Otras soluciones FOSS desarrolladas**:
  - `rop3`: `https://github.com/reverseame/rop3`
  - `Chitón`: `https://github.com/reverseame/chiton`
  - `Windows Memory Extractor`: `https://github.com/reverseame/windows-memory-extractor`
  - `IM Artifact Finder`: `https://github.com/reverseame/instant-messaging-artifact-finder`
  - `EvalMe`: `https://github.com/reverseame/EvalMe`
  - `Secure_Socket`: `https://github.com/reverseame/Secure_Socket`
  - `pinVMShield`: `https://github.com/reverseame/pinVMShield`
- **Licencias GNU/GPL3.0 y GNU/AGPL3.0**

Universidad Zaragoza

Conclusiones

Desventajas

- Modelo de “colaboración” con FOSS actual **poco reactivo**
- **Poca interacción de/desde la comunidad** (más allá de *stars*/*watchings*)
- Muchas herramientas derivadas de trabajos de investigación
- **Dificultad de gestionar** *issues* (al final, no somos una empresa desarrolladora)

Ventajas

- **Permite posicionarnos** *(conocen qué sabemos hacer)*
- **Posibilidad de amplia difusión y mejora** (por la comunidad)
- **Modelo de negocio basado en adaptaciones para empresas**

Universidad Zaragoza
1542

Experiencias propias en la contribución a proyectos de software libre: Volatility

Ricardo J. Rodríguez

Universidad Zaragoza

Dept. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza

13 de mayo, 2023

esLibre
Zaragoza, España