

Capturar Memoria RAM de Windows

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: www.ReYDeS.com :- Correo: ReYDeS@gmail.com

Jueves 29 de Junio 2023

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE)

Más de 19 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

 <https://www.linkedin.com/in/alonsocaballeroquezada/>



 https://twitter.com/Alonso_ReYDeS

 <https://www.youtube.com/c/AlonsoCaballero>

 <https://www.facebook.com/alonsoreydes/>

 https://www.instagram.com/alonso_reydes/

 reydes@gmail.com  <https://www.reydes.com>

 +51 949 304 030  @ReYDeS



RAM

RAM (Memoria de Acceso Aleatorio) es el hardware de un dispositivo de cómputo, donde el sistema operativo (SO), programas de aplicación, y datos usándose actualmente para el procesador del dispositivo pueda accederlos rápidamente. RAM es la memoria principal en una computadora. Es más rápido para leer y escribir comparado a otros tipos de almacenamiento, como un disco duro, unidad de estado sólido, o unidad óptica.

La RAM es volátil. Eso significa los datos se retienen en esta mientras la computadora está encendida, pero se pierden cuando la computadora se apaga. Cuando se reinicia la computadora, el sistema operativo y otros archivos se vuelven a cargar en la RAM, generalmente desde un dispositivos de almacenamiento como un disco duro o disco de estado sólido.

Forense de Memoria

El forense a la memoria es un área importante y crucial durante un proceso de investigación forense. Siendo en la actualidad una habilidad requerida para todo profesional en respuesta de incidentes y forense digital.

La RAM puede proporcionar; y de hecho proporciona; información muy valiosa sobre aquello lo cual se ha suscitado en un sistema, en un punto del tiempo determinado.

También podría potencialmente revelar rastros detallados, los cuales están relacionados con la actividad de aquello ocurrido, lo cual permitiría conocer diferentes detalles relacionados con un incidente.

Como toda tecnología, desde la perspectiva forense, tiene beneficios, como también inconvenientes.

Herramientas para Adquisición

Antes de ir hacia la etapa de análisis forense, se requiere evaluar la manera de obtener una imagen de la RAM.

Existen diversas herramientas disponibles factibles de ser utilizadas para lograr esto.

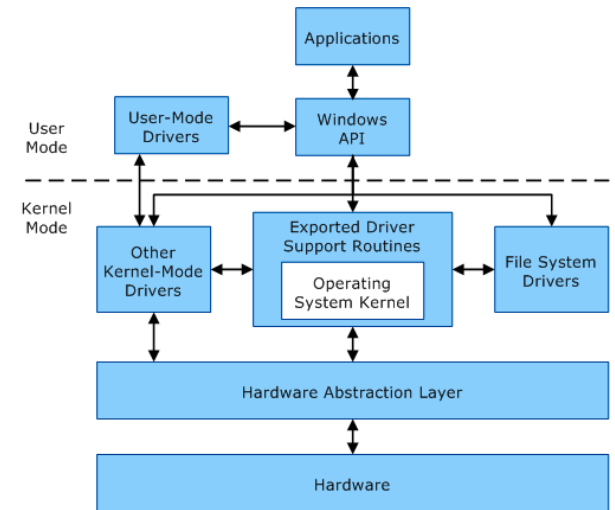
Resulta importante resaltar y recordar; cualquier herramienta seleccionada dejará inevitablemente rastros sobre el sistema bajo investigación, esta es la razón por cual nunca se instala ninguna herramientas de adquisición sobre el sistema (a menos por alguna razón sea inevitablemente necesario).

Siempre se debe documentar todos los procedimientos realizadas, así la evidencia será aceptada, y no debatida.

Modo Usuario y Modo Kernel

Un procesador en una computadora ejecutando Windows tiene dos modos diferentes: modo usuario y modo kernel.

El procesador conmuta entre estos dos modos, dependiendo de cual código se ejecuta en el procesador. Las aplicaciones se ejecutan en modo usuario, y los componentes núcleo del sistema operativo se ejecutan en modo kernel. Aunque muchos controladores se ejecutan en modo kernel, algunos pueden ejecutarse en modo usuario.



* User mode and kernel mode:

<https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode>

Espacio de Usuario y Espacio del Sistema

Windows proporciona a cada aplicación en modo usuario un bloque de direcciones virtuales. Esto es conocido como espacio de usuario de la aplicación.

El otro gran bloque de direcciones, conocido como espacio de sistema o espacio kernel, no puede ser directamente accedido por la aplicación.

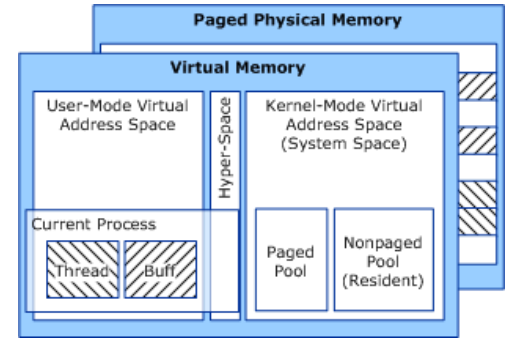
* User Space and System Space:

<https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/user-space-and-system-space>

Descripción del Espacio de Memoria Windows

La siguiente imagen ilustra los espacios de memoria virtual de sistemas operativos basados en NT, y su relación hacia la memoria física del sistema

La memoria virtual es respaldada por memoria física paginada, y un rango de direcciones virtuales puede ser respaldada por páginas de memoria física no contiguas. Una memoria virtual del espacio del usuario, y una memoria del espacio del sistema, asignado desde un grupo paginado siempre son paginables. Cualquier código del espacio de usuario o dato, puede ser paginado hacia un almacenamiento secundario en cualquier momento, incluso mientras se ejecuta el proceso.



* Overview of Windows Memory Space:

<https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/overview-of-windows-memory-space>

Curso Virtual Fundamentos Forense Digital

 Sitio Web:

www.reydes.com

 Correo:

reydes@gmail.com

Más Información:

https://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital

Alonso Eduardo Caballero Quezada :- Sitio web: www.reydes.com :- Correo: reydes@gmail.com

Fundamentos de Forense Digital

Domingos 2 y 9 de Julio del 2023. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



Presentación

El forense digital actualmente es utilizado en diversas áreas tecnológicas, no únicamente para intentar atrapar ciberdelincuentes pululando en Internet. Es utilizado en ámbitos como la captura de inteligencia, pues dada la rápida explotación de información residente en teléfonos móviles y otros tipos de dispositivos, ayuda a las fuerzas legales a identificar y neutralizar a los ciberdelincuentes. Puede ser también utilizado en litigios civiles y penales, pues ahora todos los documentos son escritos en ceros y unos, siendo almacenados en discos duros u otros dispositivos de almacenamiento. El forense digital ayuda a combatir el surgimiento masivo del cibercrimen, siendo utilizado para proteger a compañías, organizaciones, y gobiernos.

Objetivos

Este curso enseña a los participantes los fundamentos del forense digital, asumiendo el participante tiene aún mínimos conocimientos, o está algo familiarizado con el funcionamiento de computadoras y otros dispositivos digitales. Se abarcan temas teóricos del ámbito forense, donde se exponen también conceptos técnicos importantes para el desarrollo de los temas posteriormente explicados. Se detallan temas relacionados al laboratorio forense, como también las herramientas utilizadas durante todo el proceso forense, lo cual incluye la identificación, captura, preservación, análisis, y presentación de evidencia digital.

Demostraciones

The image shows two windows from a Windows operating system. The left window is a command prompt titled "Administrator: cmd - winpmem_mini_x64_rc2.exe F:\RAM_winpmem.raw". It displays the execution of the winpmem tool, which extracts a driver, loads it, and generates a RAW image of RAM. The output includes memory ranges, acquisition mode, and padding details.

```
Administrator: cmd - winpmem_mini_x64_rc2.exe F:\RAM_winpmem.raw
E:\RAM_Tools\winpmem>winpmem_mini_x64_rc2.exe F:\RAM_winpmem.raw
WinPmem64
Extracting driver to C:\Users\homero\AppData\Local\Temp\pme429F.tmp
Driver Unloaded.
Loaded Driver C:\Users\homero\AppData\Local\Temp\pme429F.tmp.
Deleting C:\Users\homero\AppData\Local\Temp\pme429F.tmp
The system time is: 14:23:03
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AA000
4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xDFEED000
Start 0x100000000 - Length 0x202000000
max_physical_memory_ 0x120200000
Acquisition mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
- length: 0x1000
00% 0x00000000 .
copy_memory
- start: 0x1000
- end: 0x9f000
00% 0x00001000 .
Padding from 0x0009f000 to 0x00100000
pad
- length: 0x61000
00% 0x0009f000 .
copy_memory
- start: 0x100000
- end: 0x102000
00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
- length: 0x1000
00% 0x00102000 .
copy_memory
- start: 0x103000
- end: 0xdfff0000
00% 0x00103000 .....
```

The right window is a File Explorer titled "KINGSTON (F:)" showing the contents of the drive. A file named "RAM_winpmem.raw" is visible, with a size of 101,724,160 bytes. The drive also shows a partition of 2.168.0.10 (S:) and a partition of 68.0.10 (X:).

Name	Date modified	Type
RAM_winpmem.raw		RAW File

Summary of F:\
3 09:23 AM 101,724,160 RAM_winpmem.raw
1 File(s) 101,724,160 bytes
0 Dir(s) 61,367,681,024 bytes free

Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético

https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Curso Virtual Hacking con Kali Linux

https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence

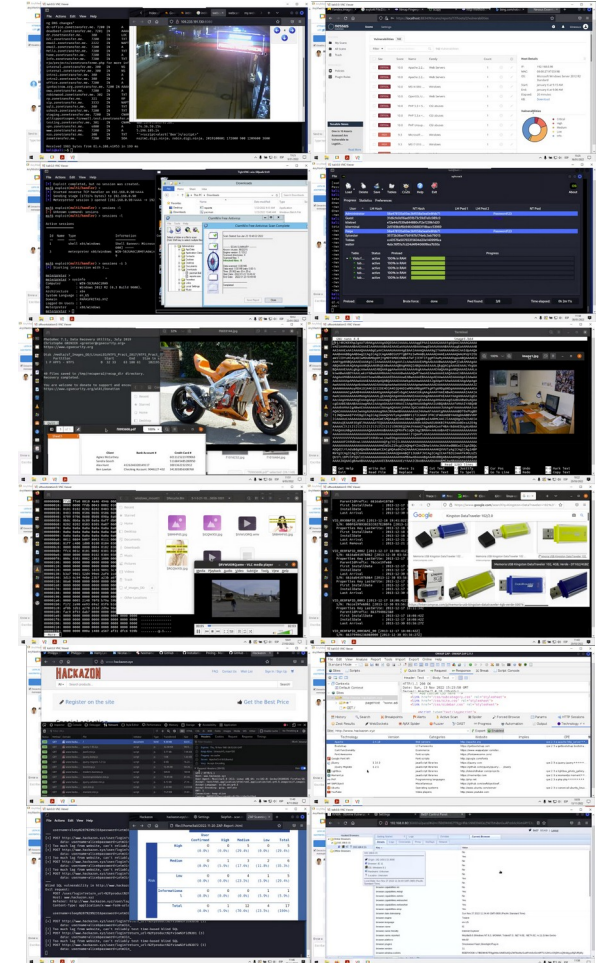
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes

https://www.reydes.com/d/?q=Curso_Forense_de_Red

Y todos los cursos virtuales:

<https://www.reydes.com/d/?q=cursos>



Más Contenidos

Videos de 85 webinars gratuitos

<https://www.reydes.com/d/?q=videos>

Diapositivas de los webinars gratuitos

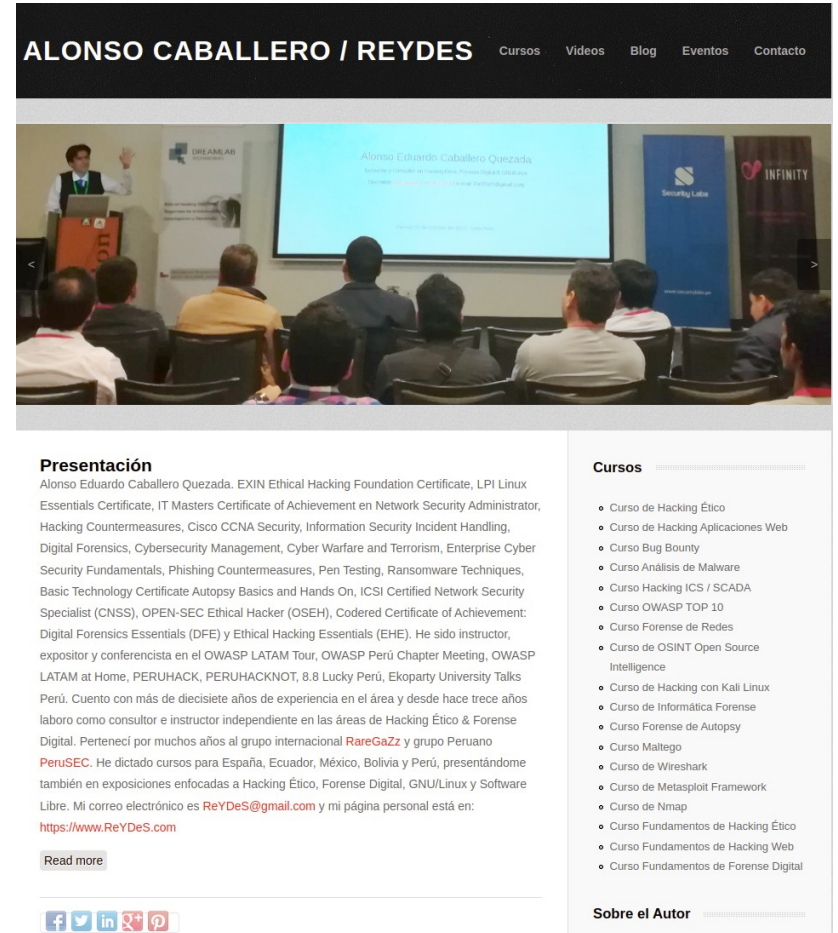
<https://www.reydes.com/d/?q=eventos>

Artículos y documentos publicados

<https://www.reydes.com/d/?q=documentos>

Blog sobre temas de mi interés

<https://www.reydes.com/d/?q=blog/1>



ALONSO CABALLERO / REYDES Cursos Videos Blog Eventos Contacto

Alonso Eduardo Caballero Quezada
EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenezco por muchos años al grupo internacional **RareGazZ** y grupo Peruano **PeruSEC**. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: <https://www.ReYDeS.com>

[Read more](#)

[f](#) [t](#) [in](#) [+](#) [p](#)

Presentación

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenezco por muchos años al grupo internacional **RareGazZ** y grupo Peruano **PeruSEC**. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: <https://www.ReYDeS.com>

Cursos

- Curso de Hacking Ético
- Curso de Hacking Aplicaciones Web
- Curso Bug Bounty
- Curso Analysis de Malware
- Curso Hacking ICS / SCADA
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de OSINT Open Source Intelligence
- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso Forense de Autopsy
- Curso Maltego
- Curso de Wireshark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital

Sobre el Autor

Capturar Memoria RAM de Windows

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: www.ReYDeS.com :- Correo: ReYDeS@gmail.com

Jueves 29 de Junio 2023