

RECUPERACION DE INFORMACION

Realizado por: Luis Carlos Arevalo Ocampo

Docente: Ing. Dr. Carlos Enrique López Rodríguez

TARAPOTO - PERU

Para iniciar el proceso de recuperación de información, utilicé una máquina virtual con el sistema operativo Linux. Además, implementé dos herramientas de Kali Linux: ExifTool y DiffPDF, para analizar los metadatos y comparar las modificaciones de los archivos.

ExifTool

FxifTool poderosa es una herramienta de línea de comandos utilizada para leer, escribir y editar metadatos en archivos de imagen, audio, video y otros formatos. Desarrollada por Phil Harvey, ExifTool es capaz de extraer información detallada como la fecha de creación, ajustes de la cámara, software utilizado y muchos otros datos embebidos en los archivos. Esta herramienta es especialmente útil en el análisis forense digital y la recuperación de datos, ya que permite obtener información valiosa sobre el historial y las características de un archivo.

DiffPDF

DiffPDF es una herramienta gráfica diseñada para comparar visualmente archivos PDF. Permite identificar las diferencias entre dos documentos en términos de texto. apariencia y DiffPDF estructura. resalta las modificaciones realizadas entre las versiones de un archivo, facilitando la revisión de cambios y actualizaciones. Esta herramienta es esencial para verificar la integridad de documentos y asegurar que no se realizado alteraciones han no autorizadas.

Pasos para la recuperación de la información

1. Inicia la máquina virtual y abre Kali Linux.



2. Una vez estando en el Kali Linux. Creamos una carpeta donde se almacenará los dos documentos que se revisara, en este caso estarán en una carpeta llamada "AUDITORIA"



 Antes de instalar cualquier paquete, es una buena práctica asegurar de que EL sistema este actualizado. Abre una terminal y ejecuta el siguiente comando:



 Dentro de Kali Linux, abre el terminal y procede a instalar la primera herramienta, "ExifTool". Se ejecuta el siguiente comando en la terminal: - sudo apt-get install exiftool



5. Para extraer metadatos de los documentos en PDF, primero ingresaremos a la carpeta donde se encuentran los documentos.



6. Ahora, aplica el siguiente comando para extraer los metadatos de los documentos en PDF utilizando ExifTool:

exiftool AUDITORIA/non	nbre del	documento.pdf
		_ /

<pre>(root@kal1)-[/home/kal1/Des # exifted] TAREA\ CONTRATO\ I</pre>	ktop/AUDITORIA] MPUTADO.ndf
ExifTool Version Number	: 12 76
Eilo Namo	, TAREA CONTRATO INDUITADO pdf
Dimostony	. TAREA CONTRATO IMPOTADO.put
File Size	 . 110 kp
File Size	: 110 KB
File Modification Date/Time	: 2024.00.20 23.23.24-04.00
File Access Date/Time	: 2024.00.27 00.24.24-04.00
File Inode Change Date/Time	: 2024:00:27 00:24:23-04:00
File Permissions	: -rw-rr
File Type	: PDF
File Type Extension	: pat
MIME Type	: application/pdf
PDF Version	: 1.5
Linearized	: No
Page Count	: 5
Language	: es-PE
lagged PDF	: Yes
Author	: Enrique
Creator	: Microsoft® Word 2016
Create Date	: 2020:10:26 00:40:13-05:00
Modify Date	: 2020:10:26 00:40:13-05:00
Producer	: Microsoft® Word 2016
(root@kali)-[/home/kali/Des	
# exifted] TAREA\ CONTRATO\ A	GRAVTADO. ndf
ExifTool Version Number	• 12.76
File News	. 12.70
FILE NAME	· TAREA CONTRATO AGRAVIADO odf
File Name Directory	: TAREA CONTRATO AGRAVIADO.pdf
File Name Directory File Size	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB
File Name Directory File Size File Modification Date/Time	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00
File Name Directory File Size File Modification Date/Time File Access Date/Time	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00
File Name Directory File Size File Modification Date/Time File Access Date/Time File Toode Change Date/Time	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-r-r-r
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-r : PDF
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension	: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MTMF Type	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr- : PDF : pdf : application/pdf</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type File Type PDF Version	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf : application/pdf : 1.5</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf : application/pdf : 1.5 : No</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf : application/pdf : 1.5 : No : 5</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr- : PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF Author	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr PDF : PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes : Enrigue</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF Author Creator	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes : Enrique : Microsoft® Word 2016</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF Author Creator Create Date	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes : Enrique : Microsoft® Word 2016 : 2020:10:26 00:41:27-05:00</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF Author Creator Create Date Modify Date	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes : Enrique : Microsoft® Word 2016 : 2020:10:26 00:41:27-05:00 : 2020:10:26 00:41:27-05:00</pre>
File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type PDF Version Linearized Page Count Language Tagged PDF Author Creator Create Date Modify Date Producer	<pre>: TAREA CONTRATO AGRAVIADO.pdf : . : 112 kB : 2024:06:26 23:23:24-04:00 : 2024:06:27 00:24:23-04:00 : 2024:06:27 00:24:23-04:00 : -rw-rr : PDF : pdf : application/pdf : 1.5 : No : 5 : es-PE : Yes : Enrique : Microsoft® Word 2016 : 2020:10:26 00:41:27-05:00 : 2020:10:26 00:41:27-05:00 : Microsoft® Word 2016</pre>

- 7. Análisis de los resultados obtenidos
 - 7.1. Fecha de creación (Create Date):
 - TAREA CONTRATO IMPUTADO.pdf: 2020:10:26 00:40:13-05:00
 - TAREA CONTRATO AGRAVIADO.pdf: 2020:10:26 00:41:27-05:00

La fecha de creación del documento "TAREA CONTRATO IMPUTADO.pdf" es anterior a la de "TAREA CONTRATO AGRAVIADO.pdf". Esto significa que "TAREA CONTRATO IMPUTADO.pdf" fue creado primero.

7.2. Tamaño del archivo (File Size):

- TAREA CONTRATO IMPUTADO.pdf: 110 kB
- TAREA CONTRATO AGRAVIADO.pdf: 112 kB

Aunque el tamaño del archivo de "TAREA CONTRATO IMPUTADO.pdf" es ligeramente menor, esto no es un factor decisivo para determinar cuál es el original.

7.3. Fecha de modificación (Modify Date):

• Ambas fechas de modificación coinciden con sus respectivas fechas de creación, lo cual indica que no ha habido modificaciones posteriores desde su creación.

7.4. Conclusión

Basándonos en la fecha de creación, el documento "TAREA CONTRATO IMPUTADO.pdf" podemos decir que es el documento original, ya que fue creado primero. La diferencia en el tamaño del archivo es mínima y no influye significativamente en la determinación de la originalidad del documento.

 Ahora, vamos a comparar los documentos utilizando la herramienta DiffPDF. Para ello, primero instalaremos la herramienta desde el terminal de Linux utilizando el siguiente comando:

 sudo apt-get install diffpdf



9. Para comparar dos archivos PDF, usa el siguiente comando, reemplazando archivo1.pdf y archivo2.pdf con los nombres de los archivos que deseas comparar. Luego se abrirá una interfaz grafica donde podremos ver las diferencias entre los dos archivos PDF.

1				DHIPDF			
File #1	TAREA CONTRATO AGRAVIADO.pdf Pages: 1-5		File #2	TAREA CONTRATO IMPUTADO.pdf Pages: 1-5		Margins Cont	rols
			_			Controls	8
	(a)			(@)		Compare: Word	s •
	TAREA: PERITAJE INFORMÁTICO	Channed the First field have di		TAREA: PERITAJE INFORMÁTICO		View: 2 vs. 2 • 1	
		document's page that				Show: «Highligh	iting» *
	Contrato de Soporte y Mantenimiento de Software	corresponds to the page shown in the View		Contrato de Soporte y Mantenimiento de Software		← Previo <u>u</u> s	→ Ne <u>x</u> t
	inte	Difference combobox.		Enhe		Zoom:	100 %
1	BLINGENEROS ASOCIADOS SAC, con RUC: 111111111, y con domicilio Jr. Auditoria S/N Tarapoto, , en delorite el PROVEEDOR		1	RLINGENEERDEADOCLADOGEAC, con EUC: 111111111, y con domicilio Jr. Auditorio 5(N Taropoto, , en obstante el PROVEEDOR		4 differ 5/5 comp	ared
,	1			Y			
,	SE con RUC: 222222222, y can domicilia en Amorarca S/N, Tarapolo, en adelante el CUENTE.			RSI con RUC: 222222222, y can domicilio en Amorarca S/N, Tarapato, en adelante el CUENTE.			
1	ie conviene lo siguiente			Se conviene lo siguiente			
	Object de Controlo La Contrinue et la del control la prestacción con tante de PENEEDCE de las auroidos La Contrinue estados en la control de las prestaciones en el servicios a las productivas programa enterneticas estados en el Aseas (in control en el Control de La Control de La Control de La Control de Robert concidencies generales está bien con al acidem en el Control de La Control de L			1: Object de Controlo 11: Control en el destino del control la presención con porte de PROFEEDC de las servicas en el control en el destino de la control de la presención con porte de PROFEEDC de las presencies interneticas este control de la control de del control de la del control de la del control de la del control de la control de la control de la del control del la del control de la dela del control de la dela del			
	Caddbaced and Introduced and Caddbaced and C			C exclusione and entropy of the second secon		Log Zoning Actions	Actions
Submissi tensas, pervais de astantica tentratad a novel de doelen render lagra para solución de consultar, cesocomiento, resolución de problemas y/o notificación de problemas relacionador con el Software.			telemáticos que permiton realizar su descargo. g Área de Clientes: Mediante coneción segura o través de la web de PROVEEDOR, el CUENTE podrá			npare	
0	formaction: Acceso o los cursos de formación y tutoridas on-line, sobre diferentes aspectos reacconadocon el Scherare, Dorgenetación: Acceso o lo Brenis de videos vimonudes de PROVEEDOR.		occader a diferenteservicion (Sentor de licencolar, Ayuda on-line, información actualizada, etc.) 13. PROVEZOR prestará el Senvicio deade sus oficinas, por teliliono o por los medios que considere apropiada, dento de las horan hábies de habojo y según el calendario laboral cificat		Options	Save As	
0	Actualizactores: PROVIZOR pontró a disposición del CUINE las nuevas versiones y/o actualaciones del 50thware, de forma que las aplicaciones están siempre al día y con las mbienas perdaciones. Las actualaciones del Sottware serán totalmente arabitas y notificadas por medias			 Larves o Janves De 08:30 o 14:00 y de 15:00 o 17:00 h. / Vermes De 08:00 o 15:00 h. Li Tempo de requiveito promedio poro los consultos setá de veintículor/lo (24) horas o inferior, si bien en caso de errores de la opticación el tempo de solución del problema puede 		Help	About
periodicities can be considered one sure advected transition to advecte any provide provide point means to be interested on the periodicity of		ser mayor o incluto no tener solución o conto plazo. En estos casos PROVEEDOR: ofrecerá sugerencias para tratar de santear el error. 28. Occasionamente las actividadescriente podrán requerir una actualización del hardware		G	uit		
	PROVEDDD2 genetate a dismicial device au oficina, por tellistino por la media que considere organisato, sente a la incruta filiais esta tatoja y agan el catalonio tatorar di cata la surven ba tatoja de la falla el tatoja el tatoja en tatoja en de la tatoja de la falla el tatoja. In esta autore de la surventa de la deposición el terror de la dela tatoja de la surventa de la dela de la dela de la dela de la dela de			pora consegui un reyor mediniento dal Unitra de To estas concentracia, el CUINE debenti evaluar transcriational de obsparte antecimiento dollo indipensatoria para el CUINE tengo el Activarse soctostados o la altina vendo esotente.			
	Página 2 de 5			Págins 2 de S			
<							>
-					20	▋▉Ø▋▋₿	CTRL DEREC
	🔎 Buscar 🛛 🛁 📕 🐂	🙆 🛂 🖏	ŷ 🕻	2 🙋 💆	^ @	≥:1 27/06)	3 12024 😽 🕵

10. En la parte derecha de la interfaz, puedes observar las comparaciones que se están realizando página por página. DiffPDF resalta las diferencias encontradas en el contenido, permitiéndote identificar rápidamente las modificaciones entre los dos documentos.

Margins Contr Controls	rols		
Co <u>m</u> pare: Words •			
<u>V</u> iew: 2 vs. 2 • 1			
S <u>h</u> ow: «Highlighting»			
← Previo <u>u</u> s	→ Ne <u>x</u> t		
<u>Z</u> oom:	100 %		
4 differ 5/5 compared			

11. Además, esta herramienta también te ayuda a ver y comparar los metadatos. En la parte inferior derecha, puedes ver los metadatos de ambos archivos, como el usuario, la fecha de creación, las páginas del documento, entre otros. Esto te proporciona una visión completa de las diferencias no solo en el contenido, sino también en los atributos del archivo.



12. Ahora, se mostrarán las modificaciones que se hicieron en cada documento, página por página. DiffPDF te permite navegar por cada página y visualizar claramente las diferencias, ayudándote a identificar qué cambios se realizaron en cada sección del documento.

File # <u>1</u>	TAREA CONTRATO AGRAVIADO.pdf Pages: 1-5	File #2	TAREA CONTRATO IMPUTADO.pdf Pages: 1-5
(
Co	ontrato de Soporte y Mantenimiento de Software	c	ontrato de Soporte y Mantenimiento de Software
Ent		Err	te
T&I ode	NGENEROS ASOCIADOS SAC, con RUC: 1111111111, y con demicilio Jr. Auditoria S/N. – Tarapoto., en tante el PROVEIDOR	1M od	INGENEROS ASOCIADOS SAC, con RUC: 111111111, y con domicilo Jr. Auditoria S/N Taropoto, , en: atorie el PROVEIDOR
Y		Y	
FISI	con RUC: 222222222, y can domicilia en Amorarca \$/N, Tarapoto, en adelante el CUENTE.	PSI	con RUC: 222222222, y con domicilio en Amorarca S/N, Tarapoto, en adelante el CUENIE.
Se	conviene lo siguiente	Se	conviene lo siguiente
1.0 1.1 de inde inde 12 PRC 2.0 2.1 de	Napha di Contabili. Contributo el seguino di presente Contrato la prestacono di conto la el PONELDOF de las la avvisas mandre, desclatación y mantenimiento per asservare, el Poneto (2), el la prostaciona y programa desclataciona ponesta del contra de la contra del contra del contra del contra del del contra ponesta del contra del contra del contra del contra del contra del del contra ponesta del contra del contra del contra del contra del contra del contra del del contra ponesta del contra del del contra ponesta del contra del del contra del contra del del 2012/DEC - contra del contra del del 2012/DEC - contra del contra del contra del contra del contra del contra del contra del del 2012/DEC - contra del contra del del 2012/DEC - contra del contra	1.1 0.0 1.2 1.2 1.2 1.2 1.2 1.2 1.2 1.2 1.2 1.2	Digita di contanta
0 0 0 0 0	bacción. El por los compresentos o partenis prestricos en pro non de PRO-HEDOX por venticos dan postemana sutera conjariar o parte de Al Marco de Construcción de la postema de la mante de la mante de Construcción de la postema de la mante de Construcción de la postema de la mante de la	22 22 0 0 0 0 0	backs. Bernice compressions is significant participants do PROVIDOR El prince compression is significant participants do PROVIDOR Marco antes antes compressions antes compressions antes do prince antes dos antes participants prince antes antes compressions antes compressions antes do prince antes dos antes princessions antes compressions antes do prince antes dos antes dos antes dos antes princessions antes antes princessions antes antes princessions antes antes princessions antes ant
0 0	relacionadas son el folharde. Documenteción: Accesa o las transa de videos y manuales de /ROVEEDOR. Actualizaciones: /ROVEEDOR: pontará a disposición del CUENE! son uevas vensiones y/o actualizacione el folharde, de forma que las aplicaciones estén siencre a día y can las induinos.		MCVERDOE previsario el Jernicio belses su oficinca, por telético o por to medios que considere apropolad, entre de las Increa Nóbelas de Intropio y legal e de indicadas laboral de Informationa La Jernica Lavera Da de Balo a Idado y als 1530 a 1950 h. / Viennes De BBB o 1550 h. 24. El Territorio de reguesta parende paro las consultas seis do vienticadoro (24) horai o
D	NewOrks on a permittor vicitar ta decorga. New Clances Handbook comento againa ta transita de la vesta de MOVHEORA, et CUINTE portá decordente diferentisaministica Destina de la cencitar. A volta in-leve, información naturalizas, es 11.3. MOVHEORE permitta envicio de las del comento de la comencia de la constance la cencitar de la comencia de la comencia de la comencia de la constance (en la cavera de cititado e 4400 y esta 1850 e 1950 h. h. Verense de las de la constance en la cavera de cititado e 4400 y esta 1850 e 1950 h. h. Verense de las de la constance en la cavera de cititado e 4400 y esta 1850 e 1950 h. h. Verense de las de la constance ande e avantaciande de la conse en la cavera de cititado e 4400 y esta 1850 e 1950 h. h. Verense de las de las de las de las de entre a la verense de las de entre de las dellas de las dellas de las de entre de las dellas de las dellas de las dellas de espericial genera tadas de las de las dellas de espericial genera tadas de las dellas de las dellas dellas de las dellas dellas dellas de las dellas		de region e region de la des admontes e una popular de las de conserver-servicador de residuades presentantes de las de restrances e las des admontes e las de la
	Pfigins 2 de 3		Pagena 2 de 5





