

Muhammad Naufal Sahidan

Analisis Forensik File PDF Menggunakan Hash, Metadata dan Inspeksi Biner

<https://github.com/Sahidannopal-15>

Pendahuluan

Dalam dunia digital forensik, menjaga integritas data merupakan hal yang sangat penting karena perubahan kecil pada sebuah file dapat memengaruhi keabsahan bukti digital. Sebagai orang yang baru belajar ke digital forensik, proyek ini disusun untuk portfolio pribadi dan sekaligus menguji dan memperdalam pemahaman awal. Fokus analisis meliputi pemeriksaan hash, metadata, dan struktur biner file menggunakan tools dasar seperti hashing, ExifTool, dan HxD, dengan tujuan mengamati dan memahami keterkaitan antar komponen tersebut.

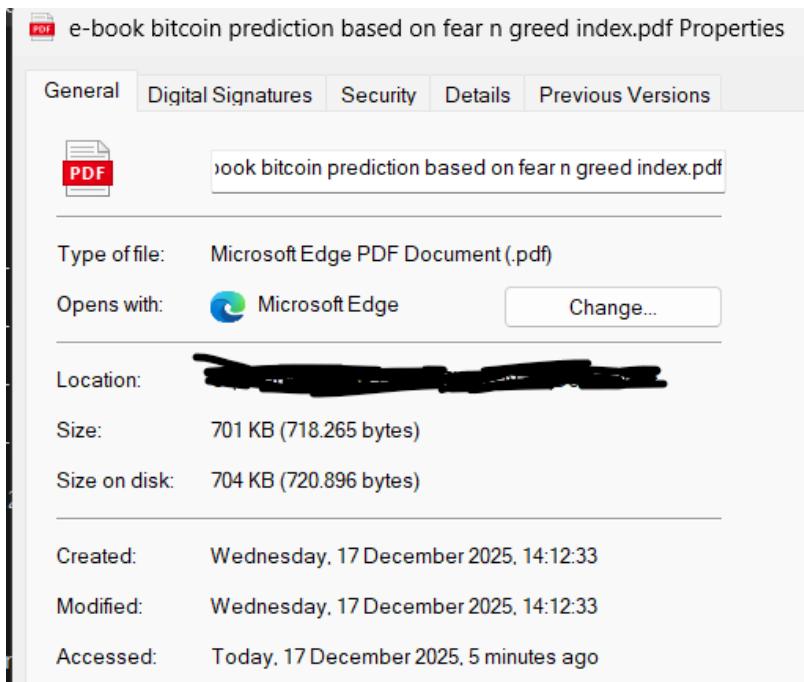
Alat yang digunakan

- Website untuk hash file
- ExifTool
- HxD

Tahap 1

Verifikasi Integritas file melalui hash

The screenshot shows a web application for calculating file hashes. At the top, there's a purple button labeled "Calculate Hash for 1 file". Below it, a radio button is selected for "Ready to calculate using SHA-256". A green "Results" button is visible. In the "Hash Results" section, a file named "e-book bitcoin prediction based on fear n greed index.pdf" is listed, showing its size as 701.43 KB and its SHA-256 hash value as 0180447225cc41a8f1eb571a889709d36e86967344fcf1f63d2c53cc17ed208b. There are download buttons for "JSON" and "CSV", and a "Copy" button next to the hash value. Below the file listing, it says "1 file processed successfully". At the bottom, it shows the algorithm used ("SHA-256") and the processing time ("Dec 17, 2025, 02:13:05 PM").



Seperti yang bisa dilihat diatas, saya telah memverifikasi file dengan menggunakan sha-256 melalui website hash dengan hash value 018d447225cc41a8f1eb571a889709d36e86967344fcf1f63d2c53cc17ed208b dan juga kita bisa mendapatkan informasi dari file awalnya seperti size dan accessed.

Tahap 2

Analisis Metadata menggunakan ExifTool

```

ExifTool Version Number : 13.31
File Name               : e-book bitcoin prediction based on fear n greed index.pdf
Directory              :
File Size               : 718 kB
Zone Identifier        : Exists
File Modification Date/Time : 2025:12:17 14:12:33+07:00
File Access Date/Time   : 2025:12:17 14:22:43+07:00
File Creation Date/Time : 2025:12:17 14:12:33+07:00
File Permissions        : -rw-rw-rw-
File Type               : PDF
File Type Extension    : pdf
MIME Type               : application/pdf
PDF Version             : 1.6
Linearized              : No
Author                 : Huang Qichuan
Create Date             : 2024:01:10 15:04:51+05:30
Modify Date             : 2024:01:16 07:40:57+01:00
Tagged PDF              : Yes
XMP Toolkit             : XMP Core 5.1.2
Metadata Date          : 2024:01:16 07:40:57+01:00
Creator Tool            : Adobe InDesign CS6 (Macintosh)
Instance ID             : uuid:87cffde5-96fc-8b46-869f-6fbdb42345ca
Original Document ID   : xmp.did:671CF283D799E7118847E8894B51C635
Document ID             : xmp.id:794E068A4F206811822AD3347B7B5182
Rendition Class        : proof:pdf
Derived From Instance ID: xmp.iid:D6CD70964E206811822AD3347B7B5182
Derived From Document ID: xmp.did:49157B7C12206811822AC9F1DA4843CF
Derived From Original Document ID: xmp.id:671CF283D799E7118847E8894B51C635
Derived From Rendition Class: default
History Action          : converted
History Parameters      : from application/x-indesign to application/pdf
History Software Agent  : Adobe InDesign CS6 (Macintosh)
History Changed         : /
History When            : 2024:01:10 15:04:51+05:30
Format                 : application/pdf
Title                  : Bitcoin price prediction based on fear \& greed index
Title (en-US)            : Bitcoin price prediction based on fear \& greed index
Creator                : Huang Qichuan
Subject                : SHS Web of Conferences 181, 02015 (2024). DOI: 10.1051/shsconf/202418102015
Producer               : Adobe PDF Library 10.0.1
Trapped                : False
Keywords               :
Page Count             : 8
-- press ENTER --

```

Pada gambar diatas banyak sekali informasi tentang metadata pdf tersebut seperti file size, author, title, create date, modify date dll.

Tahap 3

Inspeksi Struktur Biner

```

00008020 3E 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3C 72 >. <r
00008030 64 66 3A 41 6C 74 3E 0A 20 20 20 20 20 20 20 20 20 20 20 df:Alt>.
00008040 20 20 20 20 20 20 20 20 3C 72 64 66 3A 6C 69 20 78 <rdf:li x
00008050 6D 6C 3A 6C 61 6E 67 3D 22 78 2D 64 65 66 61 75 ml:lang="x-defau
00008060 6C 74 22 3E 54 68 69 73 20 73 70 61 63 65 20 73 lt">This space s
00008070 68 6F 75 6C 64 20 62 65 20 6C 65 66 74 20 62 6C hould be left bl
00008080 61 6E 6B 2C 20 65 78 63 65 70 74 20 66 6F 72 20 ank, except for
00008090 74 68 65 20 6E 61 6D 65 20 6F 66 20 74 68 65 20 the name of the
000080A0 66 69 72 73 74 20 61 75 74 68 6F 72 2E 20 28 54 first author. (T
000080B0 68 65 20 70 75 62 6C 69 73 68 65 72 20 77 69 6C he publisher wil
000080C0 6C 20 72 65 2D 74 79 70 65 20 74 68 65 20 6D 61 l re-type the ma
000080D0 69 6E 20 74 69 74 6C 65 2C 20 61 75 74 68 6F 72 in title, author
000080E0 20 6E 61 6D 65 73 20 61 6E 64 20 61 64 64 72 65 names and addre
000080F0 73 73 65 73 2E 20 50 6C 65 61 73 65 20 67 69 76 sses. Please giv
00008100 65 20 74 68 69 73 20 69 6E 66 6F 72 6D 61 74 69 e this informati
00008110 6F 6E 20 6F 6E 20 61 20 73 65 70 61 72 61 74 65 on on a separate
00008120 20 70 61 67 65 2E 29 3C 2F 72 64 66 3A 6C 69 3E page.)</rdf:li>
00008130 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 3C 2F 72 . </r
00008140 64 66 3A 41 6C 74 3E 0A 20 20 20 20 20 20 20 20 df:Alt>.
00008150 20 3C 2F 64 63 3A 74 69 74 6C 65 3E 0A 20 20 20 </dc:title>.
00008160 20 20 20 20 20 3C 64 63 3A 63 72 65 61 74 6F </dc:creato
00008170 72 3E 0A 20 20 20 20 20 20 20 20 20 20 20 20 3C r>. <
00008180 72 64 66 3A 53 65 71 3E 0A 20 20 20 20 20 20 rdf:Seq>.

```

e-book bitcoin prediction based on fear n greed index.pdf	
Offset(h)	Decoded text
0001DD10	3A 70 64 66 3D 22 68 74 74 70 3A 2F 2F 6E 73 2E :pdf="http://ns.
0001DD20	61 64 6F 62 65 2E 63 6F 6D 2F 70 64 66 2F 31 2E adobe.com/pdf/1.
0001DD30	33 2F 22 3E 0A 20 20 20 20 20 20 20 3C 70 3/">. <p
0001DD40	64 66 3A 50 72 6F 64 75 63 65 72 3E 4D 69 63 72 df:Producer>Micr
0001DD50	6F 73 6F 66 74 C2 AE 20 57 6F 72 64 20 32 30 31 osoft® Word 201
0001DD60	36 3C 2F 70 64 66 3A 50 72 6F 64 75 63 65 72 3E 6</pdf:Producer>
0001DD70	0A 20 20 20 20 20 3C 2F 72 64 66 3A 44 65 73 . </rdf:Des
0001DD80	63 72 69 70 74 69 6F 6E 3E 0A 20 20 20 20 20 20 cription>.
0001DD90	3C 72 64 66 3A 44 65 73 63 72 69 70 74 69 6F 6E <rdf>Description
0001DDA0	20 72 64 66 3A 61 62 6F 75 74 3D 22 22 0A 29 20 rdf:about=""
0001DB00	20 20 20 20 20 20 20 20 20 78 6D 6C 6E 73 3A xmlns:
0001DDC0	78 6D 70 3D 22 68 74 74 70 3A 2F 2F 6E 73 2E 61 xmp="http://ns.a
0001DDD0	64 6F 62 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 dobe.com/xap/1.0
0001DDE0	2F 22 3E 0A 20 20 20 20 20 20 20 20 3C 78 6D /">. <xm
0001DDF0	70 3A 43 72 65 61 74 6F 72 54 6F 6F 6C 3E 4D 69 pi:CreatorTools>Mi
0001DE00	63 72 6F 73 6F 66 74 C2 AE 20 57 6F 72 64 20 32 crosoft® Word 2
0001DE10	30 31 36 3C 2F 78 6D 70 3A 43 72 65 61 74 6F 72 016</xmp:Creator
0001DE20	54 6F 6F 6C 3E 0A 20 20 20 20 20 20 20 20 3C Tool>. <
0001DE30	78 6D 70 3A 43 72 65 61 74 65 44 61 74 65 3E 32 xmp:CreateDate>2
0001DE40	30 32 33 2D 31 32 2D 32 38 54 31 35 3A 34 31 3A 023-12-28T15:41:
0001DE50	32 37 2B 30 38 3A 30 30 3C 2F 78 6D 70 3A 43 72 27+08:00</xmp:Cr
0001DE60	65 61 74 65 44 61 74 65 3E 0A 20 20 20 20 20 20 eateDate>.
0001DE70	20 20 3C 78 6D 70 3A 4D 6F 64 69 66 79 44 61 <xmp:ModifyDa
0001DE80	74 65 3E 32 30 32 33 2D 31 32 2D 32 38 54 31 35 te>2023-12-28T15
0001DE90	3A 34 31 3A 32 37 2B 30 38 3A 30 30 3C 2F 78 6D :41:27+08:00</xm
0001DEA0	70 3A 4D 6F 64 69 66 79 44 61 74 65 3E 0A 20 20 p:ModifyDate>.
0001DEB0	20 20 20 20 3C 2F 72 64 66 3A 44 65 73 63 72 69 </rdf:Descri
0001DEC0	70 74 69 6F 6E 3E 0A 20 20 20 20 20 3C 72 64 ption>. <rd
0001DED0	66 3A 44 65 73 63 72 69 70 74 69 6F 6E 20 72 64 f:Description rd
0001DEE0	66 3A 61 62 6F 75 74 3D 22 22 0A 20 20 20 20 20 f:about="".
0001DEF0	20 20 20 20 20 20 20 78 6D 6C 6E 73 3A 78 6D 70 xmlns:xmp
0001DF00	4D 4D 3D 22 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 MM="http://ns.ad
0001DF10	6F 62 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F obe.com/xap/1.0/
0001DF20	6D 6D 2F 22 3E 0A 20 20 20 20 20 20 20 20 20 3C mm/">. <
0001DF30	78 6D 70 4D 4D 3A 44 6F 63 75 6D 65 6E 74 49 44 xmpMM:DocumentID
0001DF40	3E 75 75 69 64 3A 33 41 34 39 34 33 43 2D 30 >uuid:3A49434C-0

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
0001DF20	6D 6D 2F 22 3E 0A 20 20 20 20 20 20 20 20 20 3C	mm/*>. <
0001DF30	78 6D 70 4D 4D 3A 44 6F 63 75 6D 65 6E 74 49 44	xmpMM:DocumentID
0001DF40	3E 75 75 69 64 3A 33 41 34 39 34 33 34 43 2D 30	>uuid:3A49434C-0
0001DF50	33 44 46 2D 34 44 32 44 2D 41 45 46 33 2D 45 46	3DF-4D2D-AEF3-EF
0001DF60	30 39 38 35 33 45 41 36 39 46 3C 2F 78 6D 70 4D	09853EA69F</xmpM
0001DF70	4D 3A 44 6F 63 75 6D 65 6E 74 49 44 3E 0A 20 20	M:DocumentID>.
0001DF80	20 20 20 20 20 20 3C 78 6D 70 4D 4D 3A 49 6E	<xmpMM:In
0001DF90	73 74 61 6E 63 65 49 44 3E 75 75 69 64 3A 33 41	stanceID>uuid:3A
0001DFA0	34 39 34 33 34 43 2D 30 33 44 46 2D 34 44 32 44	49434C-03DF-4D2D
0001DFB0	2D 41 45 46 33 2D 45 46 30 39 38 35 33 45 41 36	-AEF3-EF09853EA6
0001DFC0	39 46 3C 2F 78 6D 70 4D 4D 3A 49 6E 73 74 61 6E	9F</xmpMM:Instan
0001DFD0	63 65 49 44 3E 0A 20 20 20 20 20 3C 2F 72 64	ceID>. </rd
0001DFE0	66 3A 44 65 73 63 72 69 70 74 69 6F 6E 3E 0A 20	f:Description>.
0001DFF0	20 20 20 20 3C 72 64 66 3A 44 65 73 63 72 69	<rdf:Descri
0001E000	70 74 69 6F 6E 20 72 64 66 3A 61 62 6F 75 74 3D	ption rdf:about=
0001E010	22 22 0A 20 20 20 20 20 20 20 20 20 20 20 20 78	"". x
0001E020	6D 6C 6E 73 3A 64 63 3D 22 68 74 74 70 3A 2F 2F	mlns:dc="http://
0001E030	70 75 72 6C 2E 6F 72 67 2F 64 63 2F 65 6C 65 6D	purl.org/dc/eleme
0001E040	65 6E 74 73 2F 31 2E 31 2F 22 3E 0A 20 20 20 20	nts/1.1/">.
0001E050	20 20 20 20 3C 64 63 3A 74 69 74 6C 65 3E 0A	<dc:title>.
0001E060	20 20 20 20 20 20 20 20 20 20 20 3C 72 64 66	<rdf
0001E070	3A 41 6C 74 3E 0A 20 20 20 20 20 20 20 20 20 20	:Alt>.

Gambar file mentah ini bisa dikatakan sangat mirip dengan isi metadata yang sudah dilakukan, seperti kemiripan pada Creator Tool, Producer, Create Date, Modify Date, Documentid.

Korelasi

a) Korelasi Hash & File

Nilai	hash
018d447225cc41a8f1eb571a889709d36e86967344fcf1f63d2c53cc17ed208b	
berfungsi untuk memverifikasi integritas file	

b) Korelasi Metadata & Struktur biner

- Pada ExifTool terdapat Producer adalah Adobe PDF Library 10.0.1 dan Creator Tool adalah Adobe InDesign CS6.
- Pada HxD terdapat Producer adalah Microsoft word 2016 dan pada Creator Tool juga Microsoft Word 2016

Analisis Korelasi = Walaupun terdapat banyak kesamaan data pada metadata dan struktur biner tetapi terdapat perbedaan pada procedur dan Creator Tool, kemungkinan yang terjadi karna file awal dibuat dengan Microsoft Word 2016 lalu author mengedit layout halaman di Adobe InDesign CS6 setelah itu mengkonversi ke Adobe PDF Library.

Analisis Akhir

Berdasarkan analisis yang telah dilakukan terhadap file "e-book bitcoin prediction based on fear n greed index.pdf" menggunakan tiga metode verifikasi seperti hash, metadata, dan struktur biner, berikut adalah kesimpulan dari setiap tahap analisis:

1. Verifikasi integritas file menggunakan hash

Hash value :

018d447225cc41a8f1eb571a889709d36e86967344fcf1f63d2c53cc17ed208b.

- Hash ini berfungsi sebagai “sidik jari digital” dari file pdf ini
- Setiap perubahan sekecil apapun pada file akan menghasilkan hash yang berbeda

2. Analisis Riwayat File: Terdapat beberapa ketidak konsistenan antara struktur biner dan metadata :

- Terdapat indikasi Editing: Ditemukan ketidak konsistenan antara struktur biner yang mencatat Microsoft Word 2016 dengan metadata akhir yang mencatat Adobe InDesign CS6.
- Analisis : Kuat dugaan file ini disusun pertama kali di Word, kemudian dipindahkan ke InDesign untuk desain layout, sebelum akhirnya dikonversi ke format PDF melalui Adobe PDF Library.
- Validasi: Pada struktur biner juga terdapat banyak data yang sama dengan metadata dan itu bisa mengonfirmasi bahwa data yang dibaca ExifTool benar-benar tertanam dalam file.