

LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIKA DIGITAL



Dosen Pengampu: Rizky Fenaldo Maulana, S.Kom., M.Kom.

Disusun Oleh :

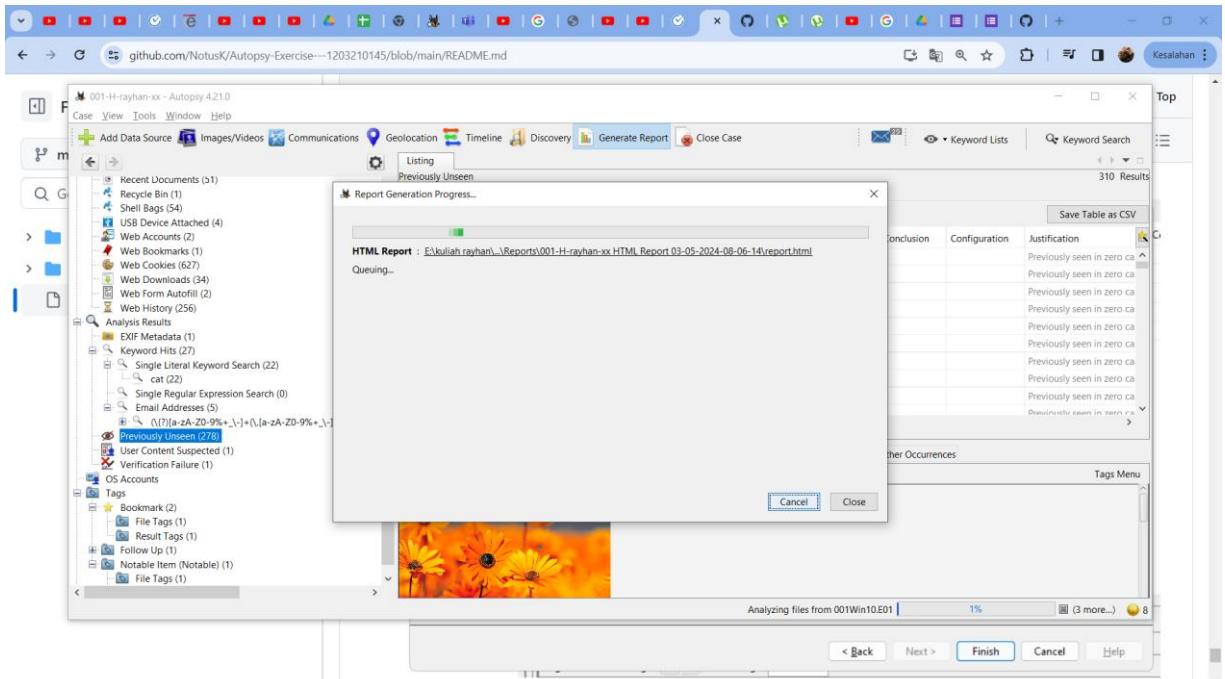
Rayhan Furqoni

1203210139

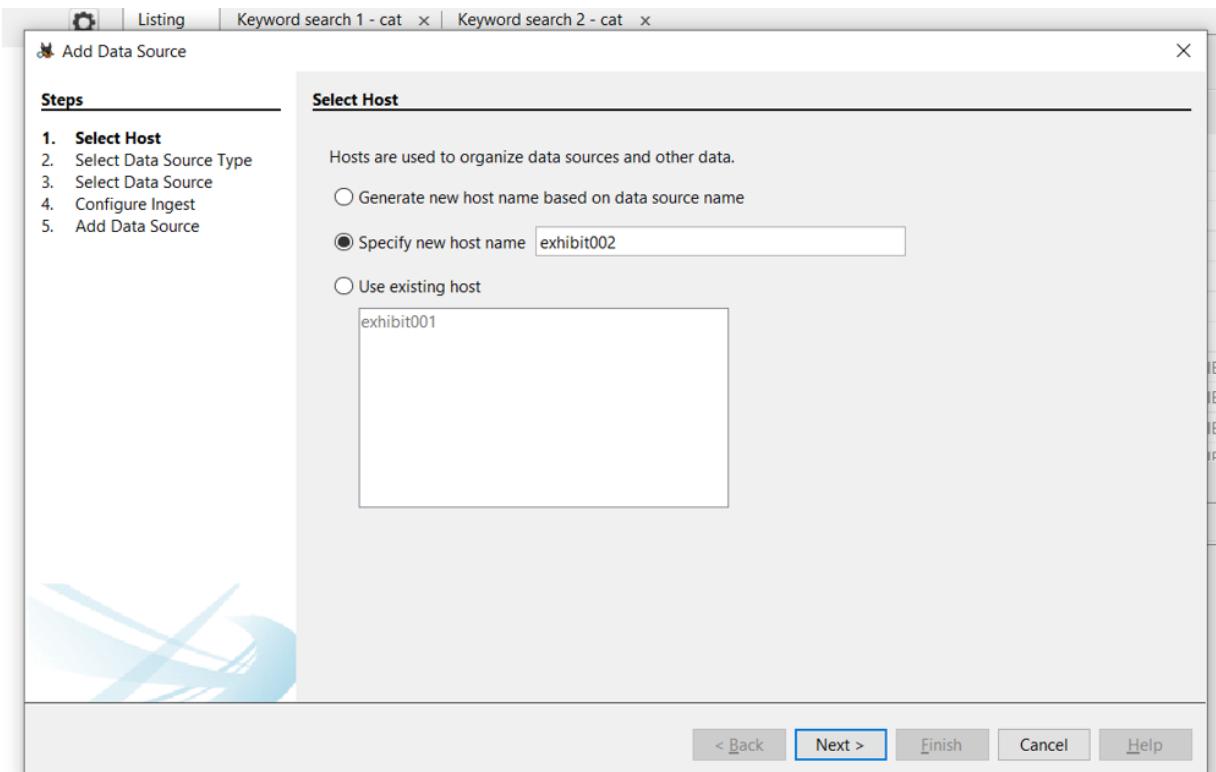
IF 01-01

**PROGRAM STUDI INFORMATIKA
FAKULTAS INFORMATIKA
TELKOM UNIVERSITY SURABAYA
TAHUN AJARAN 2023/2024**

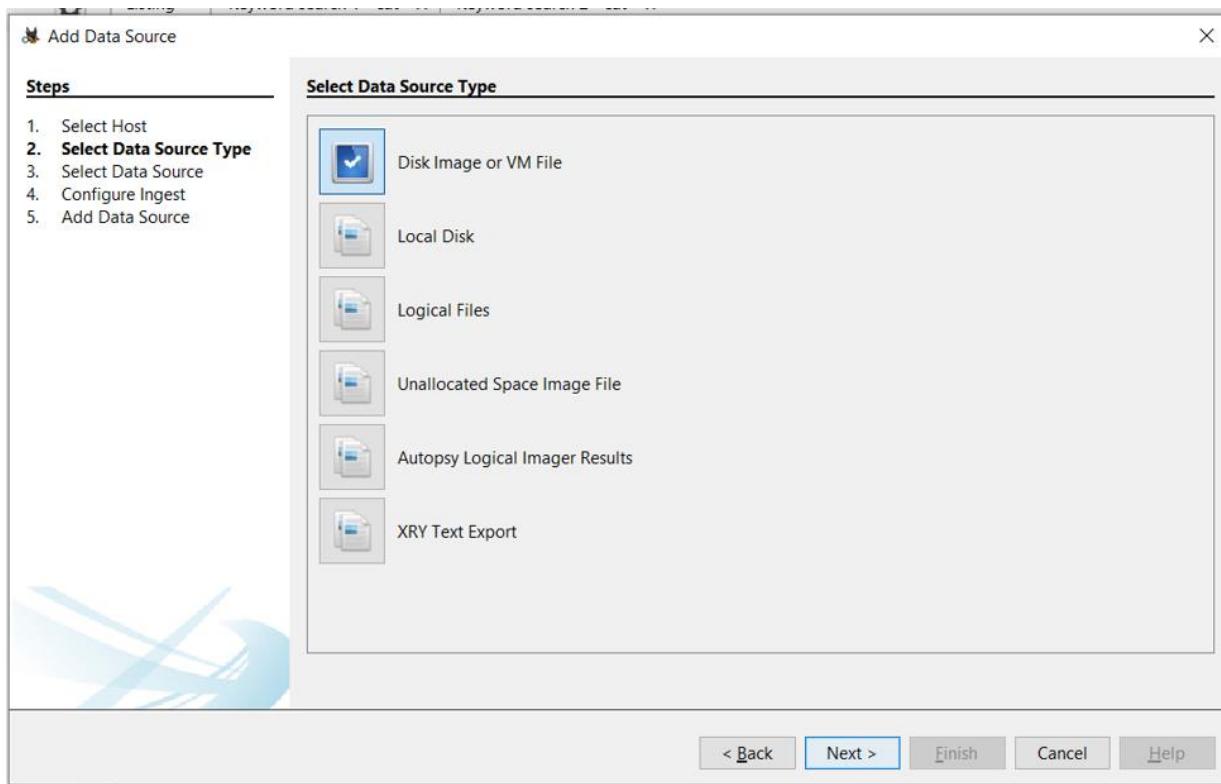
1. Add data



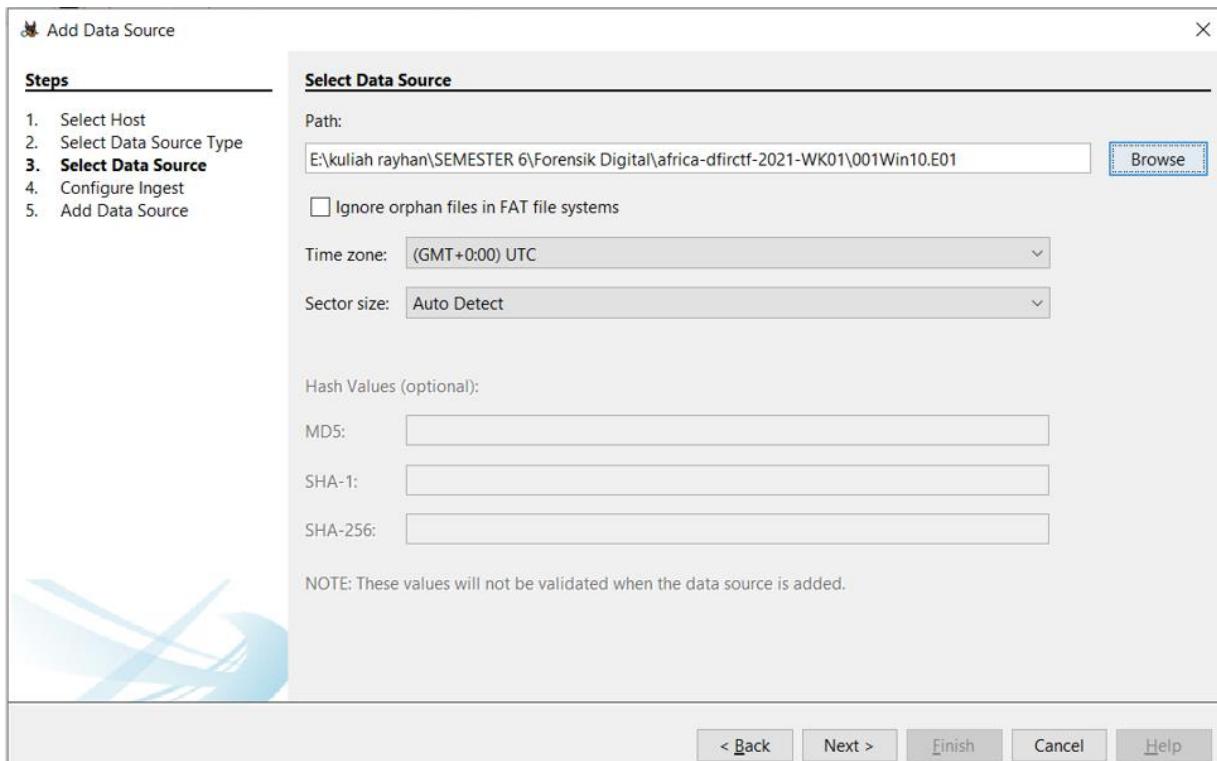
2. Select host



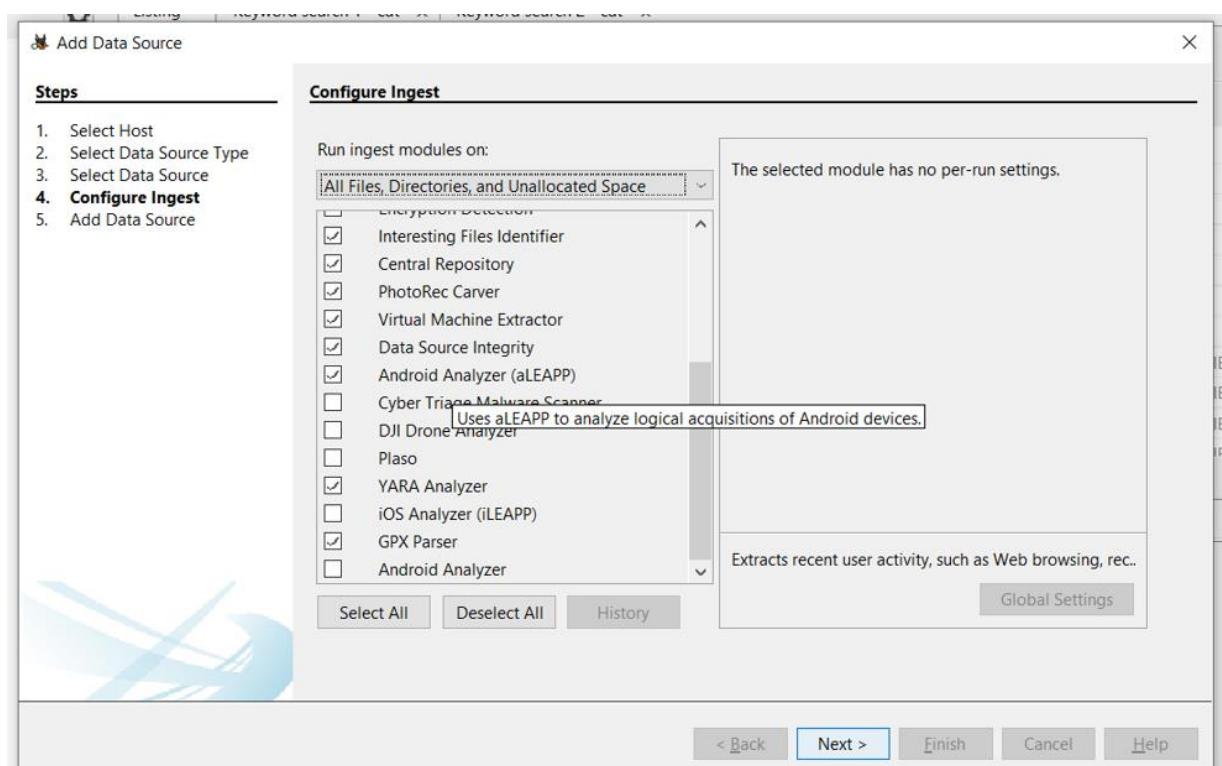
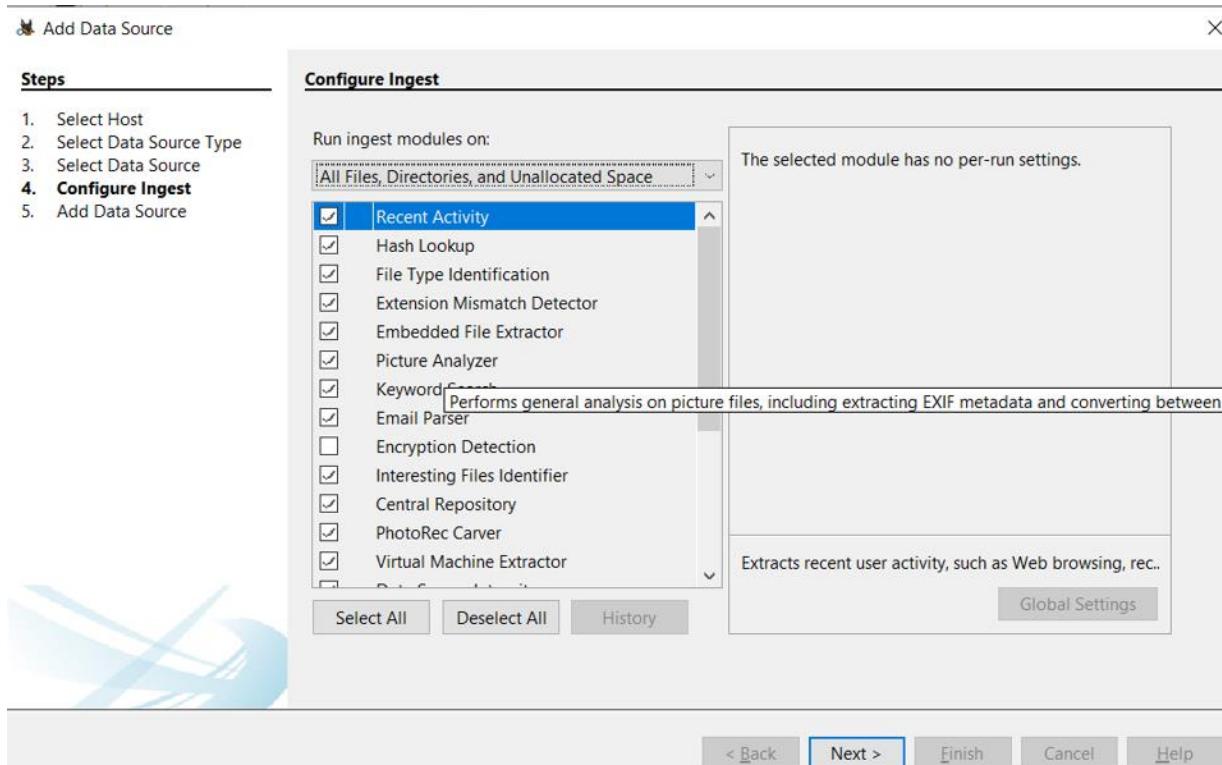
3. Pilih disk image or VM



4. Setting path file dan waktu



5. Centang kategori yang diperlukan



6. Pada Vol3 NTFS terdapat file \$MFT yang berarti vol3 merupakan C drive.

The screenshot shows the Autopsy 4.21.0 interface. The top menu bar includes Case, View, Tools, Window, Help, and several icons for adding data sources, viewing images/videos, communications, geolocation, timeline, discovery, generating reports, and closing cases. The main window displays a file listing for a volume. The listing tab is active, showing a table with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, and Size. The table lists several files, with the \$MFT file highlighted. Below the table are tabs for Thumbnail and Summary. A sidebar on the left shows Data Sources (exhibit001, exhibit002, exhibit003) and File Views (File Types, By Extension, By MIME Type, Deleted Files, MB File Size, Data Artifacts). The bottom of the screen shows a hex dump of the selected \$MFT file.

7. Pada Folder User terdapat NTUSER.DAT yang merupakan registry hive, tempat

8. Pada Installed Programs di Data Artifact menampilkan informasi aplikasi apa saja yang telah di install di sistem

The screenshot shows the Autopsy 4.21.0 interface with the 'Installed Programs' tab selected in the 'Data Artifacts' section. The results table displays various installed software programs with columns for Source Name, S, C, O, Program Name, Date/Time, and Data Source. One row is highlighted for 'Angry IP Scanner v.3.7.6'. Below the table is a detailed view of the selected item, showing its Type (Program Name), Value (Angry IP Scanner v.3.7.6), and Source(s) (001Win10.E01). Other details include Date/Time (2021-04-29 16:03:13 WIB), Source File Path (/img_001Win10.E01/vol_vol3/Windows/System32/config/SOFTWARE), and Artifact ID (-9223372036854775618).

9. Recent document

The screenshot shows the Autopsy 4.21.0 interface with the 'Recent Documents' tab selected in the 'Data Artifacts' section. The results table lists recent documents with columns for Source Name, S, C, O, Path, Date Accessed, and Data Source. The table includes entries for various files such as password lists, contact files, and configuration files, all originating from the user 'John Doe'.

10. Recycle bin

11. Shell bags folder yang diakses user

12. Usb deviced attached mengidentifikasi perangkat apa saja yang terconnect

001-H-rayhan-xx - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

USB Device Attached

Listing

Table Thumbnail Summary

Source Name S C O Date/Time Device Make Device Model Device ID Data So

SYSTEM	0		2021-04-30 02:58:36 WIB	ROOT_HUB30	48x14c8fa7&0&0	001Win1
SYSTEM	0		2021-04-30 07:46:25 WIB	LG Electronics USA, Inc. Product: 70D6	AA00000000000000873	001Win1
SYSTEM	0		2021-04-30 07:46:46 WIB	LG Electronics, Inc. LM-X420xxx/G2/G3 Android Phone (MTP/download mo. LMQ725K2c1b72a	001Win1	
SYSTEM	0		2021-04-30 02:58:36 WIB	VirtualBox USB Tablet	58xd788e13&0&0	001Win1

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: of Result

Analyzing files from 001Win10.E01 | 1% (3 more...) 8

13. Web account tempat mengetahui kamu login dmana saja

001-H-rayhan-xx - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing

Web Accounts

Table Thumbnail Summary

Source Name S C O URL Date Created Decoded URL Username Realm Domain

Login Data			http://127.0.0.1/	2021-04-29 00:30:53 WIB	127.0.0.1	Default	http://127.0.0.1/	127.0.0.1
Login Data			https://mail.protonmail.com/	2021-04-30 08:05:07 WIB	protonmail.com	Default	https://mail.protonmail.com/	protonmail

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: of Result

Analyzing files from 001Win10.E01 | 1% (3 more...) 8

14. Web cookies berisi data tentang web yang pernah kamu masukin

Autopsy 4.21.0 - 001-H-rayhan-xx

Web Cookies

Source Name	S	C	O	URL	Date Accessed	Name	Value	Program Name
Cookies	1	1	1	youtube.com	2021-04-30 03:43:55 WIB	VISITOR_INFO1_LIVE		Brave
Cookies	1	1	1	youtube.com	2021-04-30 03:43:55 WIB	YSC		Brave
Cookies	1	1	1	google.com	2021-04-30 07:19:54 WIB	CGIC		Brave
Cookies	1	1	1	google.com	2021-04-30 07:19:52 WIB	CGIC		Brave
Cookies	1	1	1	wikipedia.org	2021-04-29 23:49:43 WIB	GeoIP		Brave
Cookies	1	1	1	wikipedia.org	2021-04-29 23:49:43 WIB	WMF-Last-Access		Brave
Cookies	1	1	1	wikipedia.org	2021-04-29 23:49:43 WIB	WMF-Last-Access-Global		Brave
Cookies	1	1	1	alpinelinux.org	2021-04-29 23:44:17 WIB	_cfuid		Brave
Cookies	1	1	1	alpinelinux.org	2021-04-29 23:44:36 WIB	_fbp		Brave
Cookies	1	1	1	cybersecurityaa.com	2021-04-29 23:45:45 WIB	_cfuid		Brave

Cookie Details

- Domain: google.com
- URL: .google.com
- Name: CGIC
- Value:
- Program Name: Brave

15. Web download berisi history download file yang berisi tgl dan tempat download.

Autopsy 4.21.0 - 001-H-rayhan-xx

Web Downloads

Source Name	S	C	O	Path	URL	Date Accessed
History	1	1	1	C:\Users\John Doe\Downloads\QCSetup.exe	http://cybermencence.co.uk/software-products/QCSetup.	2021-04-29 23:46:09 WIB
History	1	1	1	C:\Users\John Doe\Downloads\SDDelete.zip	https://download.sysinternals.com/files/SDDelete.zip	2021-04-30 03:44:59 WIB
History	1	1	1	C:\Users\John Doe\Downloads\inmap-7.91-setup.exe	https://nmap.org/dist/inmap-7.91-setup.exe	2021-04-29 00:14:00 WIB
History	1	1	1	C:\Users\John Doe\Downloads\bettercap_windows_am_..	https://github.com/bettercap/bettercap/releases/downl	2021-04-29 00:16:44 WIB
History	1	1	1	C:\Users\John Doe\Downloads\WireShark-win64-3.4.e..	https://1.eu.dl.wireshark.org/win64/Wireshark-win64-3.4.2021-04-29 00:18:45 WIB	
History	1	1	1	C:\Users\John Doe\Downloads\download.jpg	data:image/jpeg;base64,/9IAAAQSKZlrgABAQAAAQAA.	2021-04-29 21:19:51 WIB
History	1	1	1	C:\Users\John Doe\Downloads\ipscan-3.7.6-setup.exe	https://github-releases.githubusercontent.com/1968850/2021-04-29 23:02:27 WIB	
History	0	1	1	C:\Users\John Doe\Downloads\filezilla_3.53.1_win64.exe	https://clie.rin.filzilla-project.org/client/FileZilla_3.53.1_2021-nd-29_23-07-14 WIB	

Table meta

key	value
mmap_status	-1
version	43
last_compat	16
early_expir...	13256701525040679

16. Web form autofill berisi data pengguna berupa username

001-H-rayhan-xx - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Web Form Autofill 2 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Name	Value	Count	Date Created	Date Accessed	Username	Program Name	Data S
Web Data				username	bettercap	1	2021-04-29 00:25:30 WIB	2021-04-29 00:25:30 WIB	Default	Google Chrome	001Wi
Web Data				username	dreammaker82	1	2021-04-30 08:04:54 WIB	2021-04-30 08:04:54 WIB	Default	Google Chrome	001Wi

Deleted Files File System (2386) All (2388)

MB File Size

Data Artifacts Chromium Extensions (52) Chromium Profiles (3) Favicon (288) Installed Programs (48) Metadata (1) Operating System Information (1) Recent Documents (51) Recycle Bin (1) Shell Bags (54) USB Device Attached (4) Web Accounts (2) Web Bookmarks (1) Web Cookies (627) Web Downloads (34) Web Form Autofill (2) Web History (256)

Analysis Results EXIF Metadata (1)

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 2 Result < >

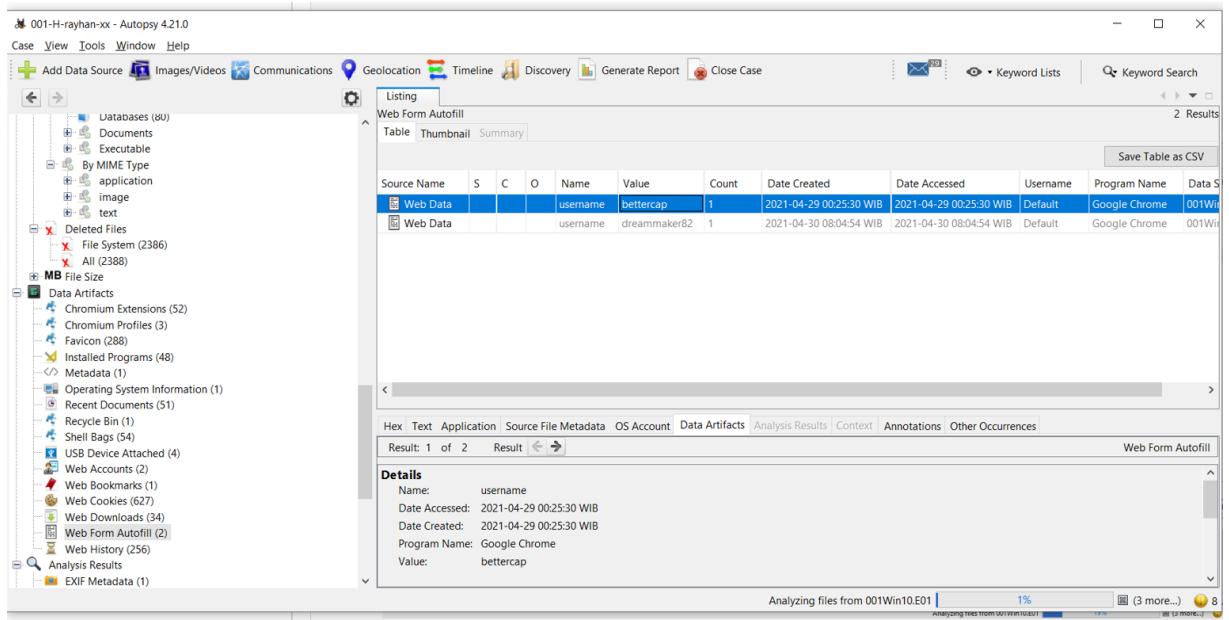
Web Form Autofill

Details

Name: username
Date Accessed: 2021-04-29 00:25:30 WIB
Date Created: 2021-04-29 00:25:30 WIB
Program Name: Google Chrome
Value: bettercap

Analyzing files from 001Win10.E01 | 1% (3 more...) 8

Analyzing files from 001Win10.E01 | 1% (3 more...) 8



17. Web history berisi rekam jejak web pengguna

The screenshot shows the Autopsy 4.21.0 interface with the 'Web History' tab selected in the top navigation bar. The main pane displays a table of web history entries. The columns are: Source Name, S, C, O, URL, Date Accessed, and Referrer URL. The table lists several entries from a 'History' source, all pointing to various YouTube URLs. A message at the bottom of the table states: 'There were 1 datasource(s) found with occurrences of the correlation value of type Domain'. The left sidebar shows a tree view of the case contents, including Databases, Documents, Executable, By MIME Type, Deleted Files, File System, MB File Size, Data Artifacts, Recent Documents, Recycle Bin, Shell Bags, USB Device Attached, Web Accounts, Web Bookmarks, Web Cookies, Web Downloads, Web Form Autofill, and a folder for 'Web History (256)'. The bottom status bar indicates 'Analyzing files from 001Win10.E01' and '1%'.

Source Name	S	C	O	URL	Date Accessed	Referrer URL
History	1			http://youtube.com/	2021-04-26 02:13:52 WIB	http://youtube.com/
History	1			https://youtube.com/	2021-04-26 02:13:52 WIB	https://youtube.com/
History	1			https://www.youtube.com/	2021-04-29 21:20:56 WIB	https://www.youtube.com/
History	1			https://www.youtube.com/	2021-04-29 21:20:56 WIB	https://www.youtube.com/
History	1			https://www.youtube.com/	2021-04-29 21:20:56 WIB	https://www.youtube.com/
History	1			https://www.youtube.com/watch?v=TQHEjj68jew	2021-04-26 02:29:16 WIB	https://www.youtube.com/watch?v=TQHEjj68jew
History	1			https://www.youtube.com/watch?v=TQHEjj68jew	2021-04-26 02:29:16 WIB	https://www.youtube.com/watch?v=TQHEjj68jew
History	1			https://www.youtube.com/	2021-04-29 21:20:56 WIB	https://www.youtube.com/
History	1			https://www.youtube.com/	2021-04-29 21:20:56 WIB	https://www.youtube.com/

18. Exif metadata berisi file jpg

The screenshot shows the Autopsy 4.21.0 interface with the 'Listing' tab selected under the 'EXIF Metadata' section. A single result is listed:

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	File Path
WelcomeScan.jpg				File	0	Not Notable			2004-04-09 15:17:00 WIB	/img_001Win10.E01

The left sidebar shows various analysis results, including 'Deleted Files', 'MB File Size', 'Data Artifacts', and 'Analysis Results' which lists 'EXIF Metadata' (1 result). The bottom status bar indicates 'Analyzing files from 001Win10.E01'.

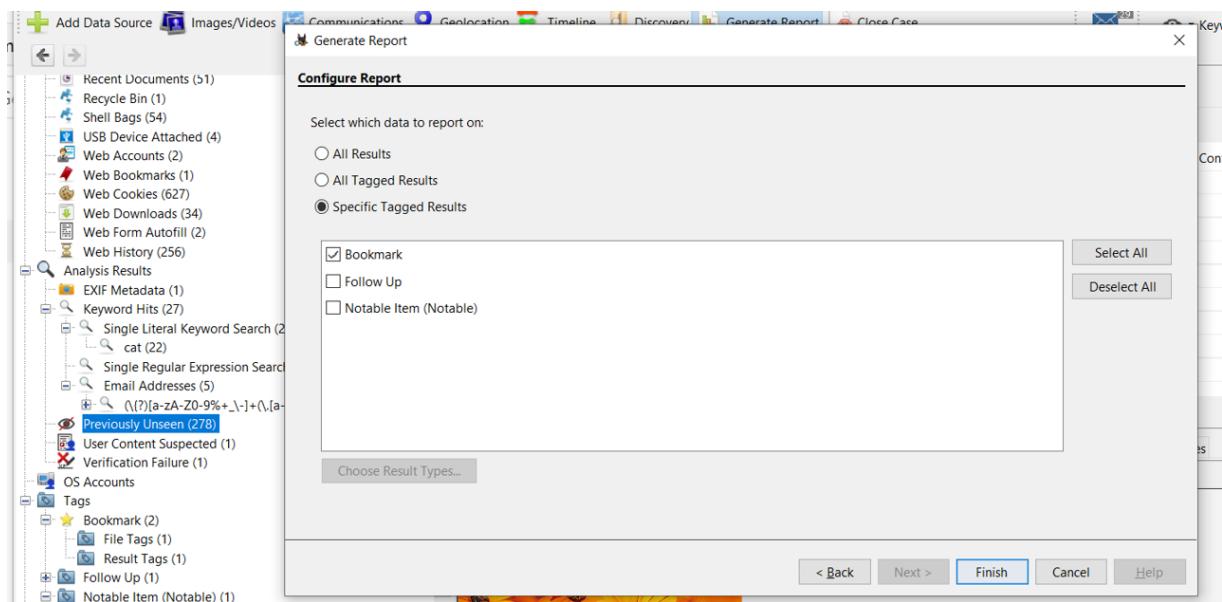
19. User content suspected file autopsy yang dibuat user

The screenshot shows the Autopsy 4.21.0 interface with the 'Listing' tab selected under the 'User Content Suspected' section. A single result is listed:

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	File Path
WelcomeScan.jpg				File	0	Unknown			EXIF metadata data exists for this file.	/img_001W...

The left sidebar shows various analysis results, including 'Recent Documents', 'USB Device Attached', and 'Analysis Results' which lists 'EXIF Metadata' (1 result), 'Keyword Hits' (27), and 'User Content Suspected' (1 result). The bottom status bar indicates 'Analyzing files from 001Win10.E01'.

20. Generate report



21. Setelah diproses kita masukkan data report ke file kasus kita

The screenshot shows the generated Autopsy Forensic Report. The left sidebar is titled 'Report Navigation' and contains links: Case Summary, Keyword Hits (0), Tagged Files (2), Tagged Images (2), and Tagged Results (0). The main content area is titled 'Autopsy Forensic Report' and shows the following details:
HTML Report Generated on 2024/03/05 03:14:00
Case: 001-H-rayhan-xx
Case Number: 001
Number of data sources in case: 1
Examiner: rayhan

Below this, there is a section titled 'Image Information'.

