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

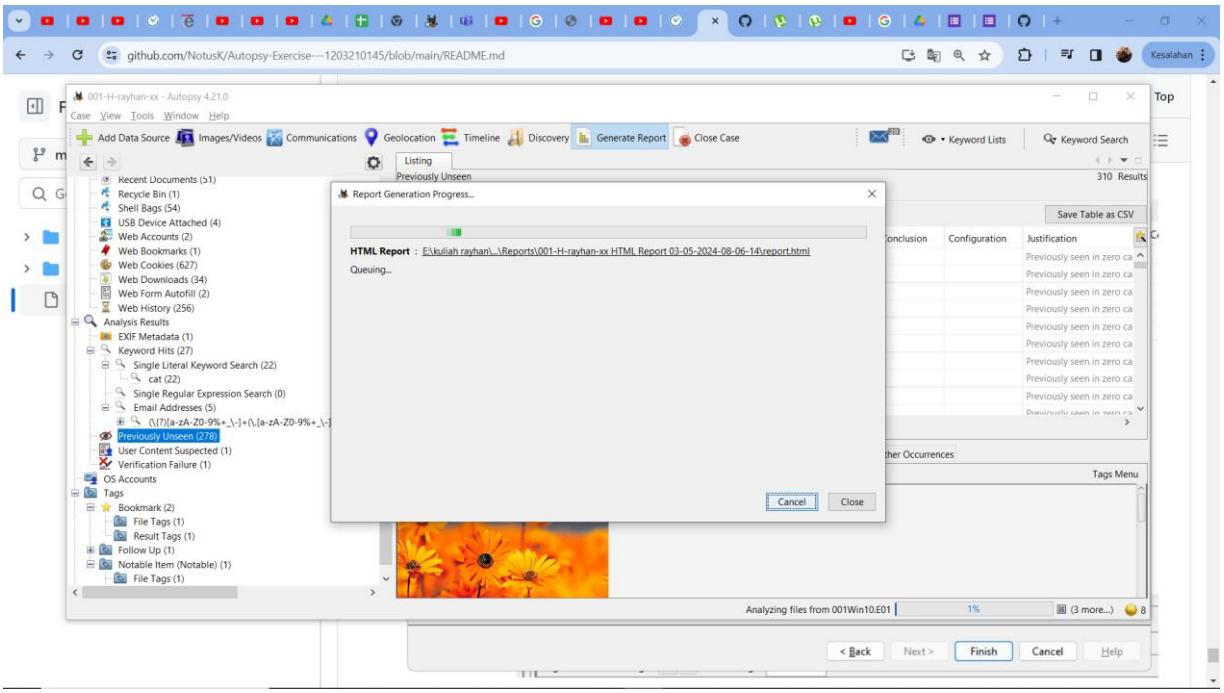
PROGRAM STUDI INFORMATIKA

FAKULTAS INFORMATIKA

TELKOM UNIVERSITY SURABAYA

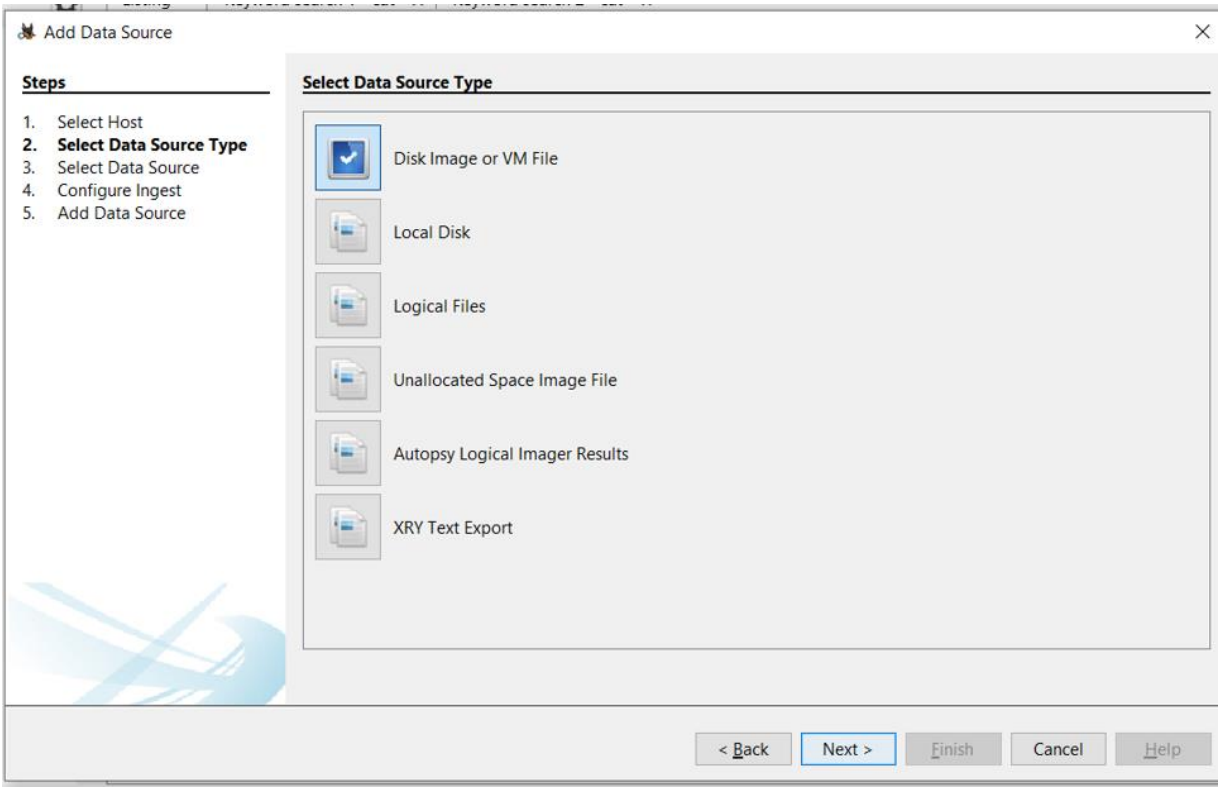
TAHUN AJARAN 2023/2024

1. Add data

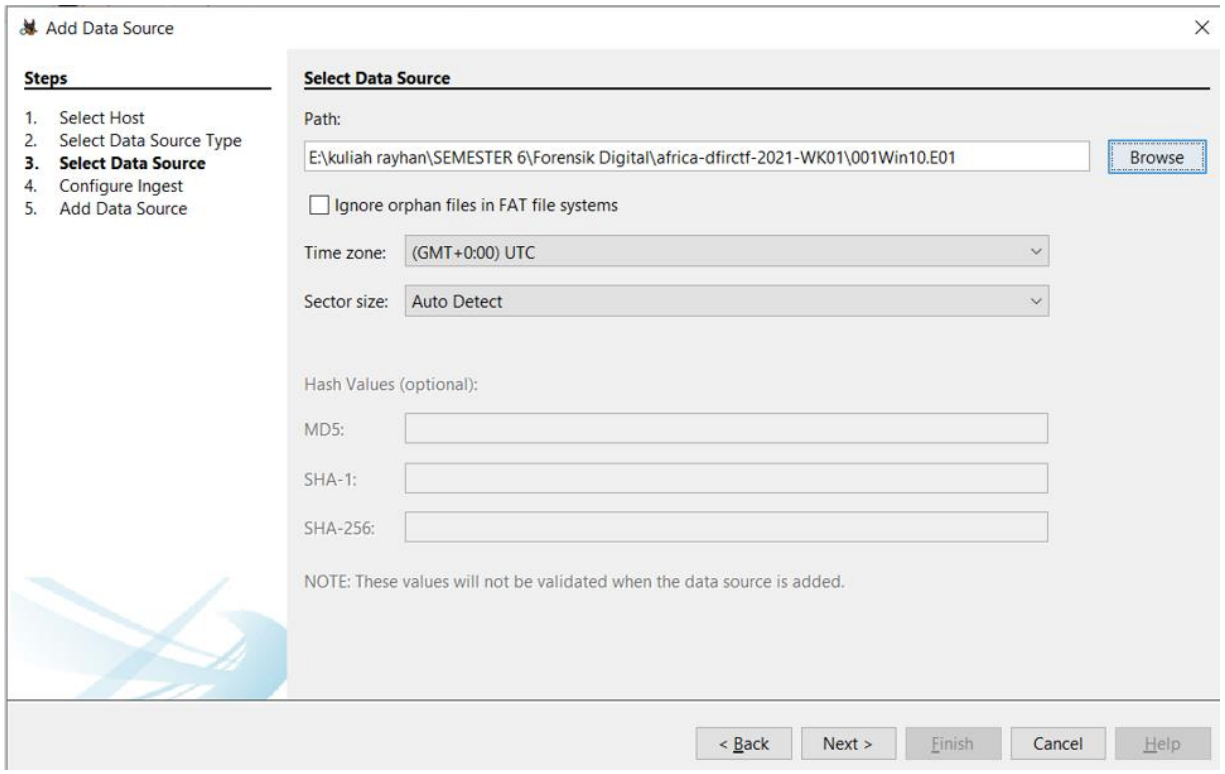


2. Select host

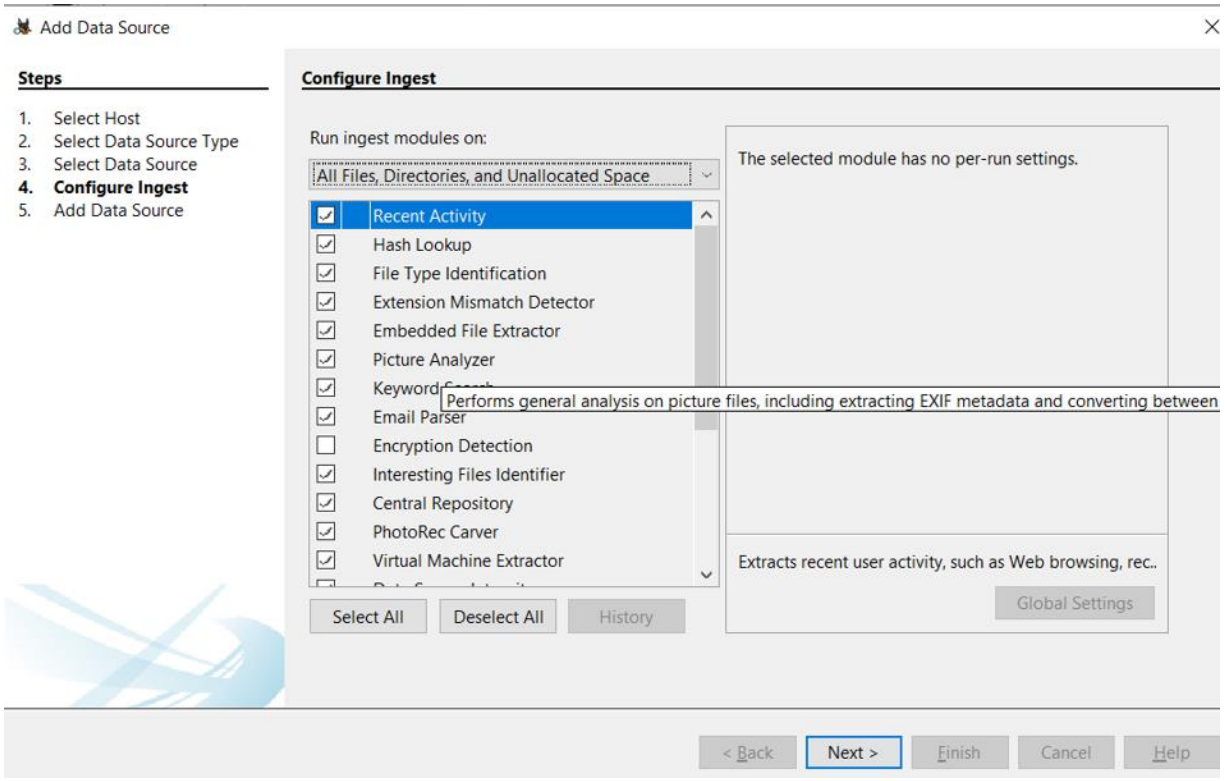
3. Pilih disk image or VM

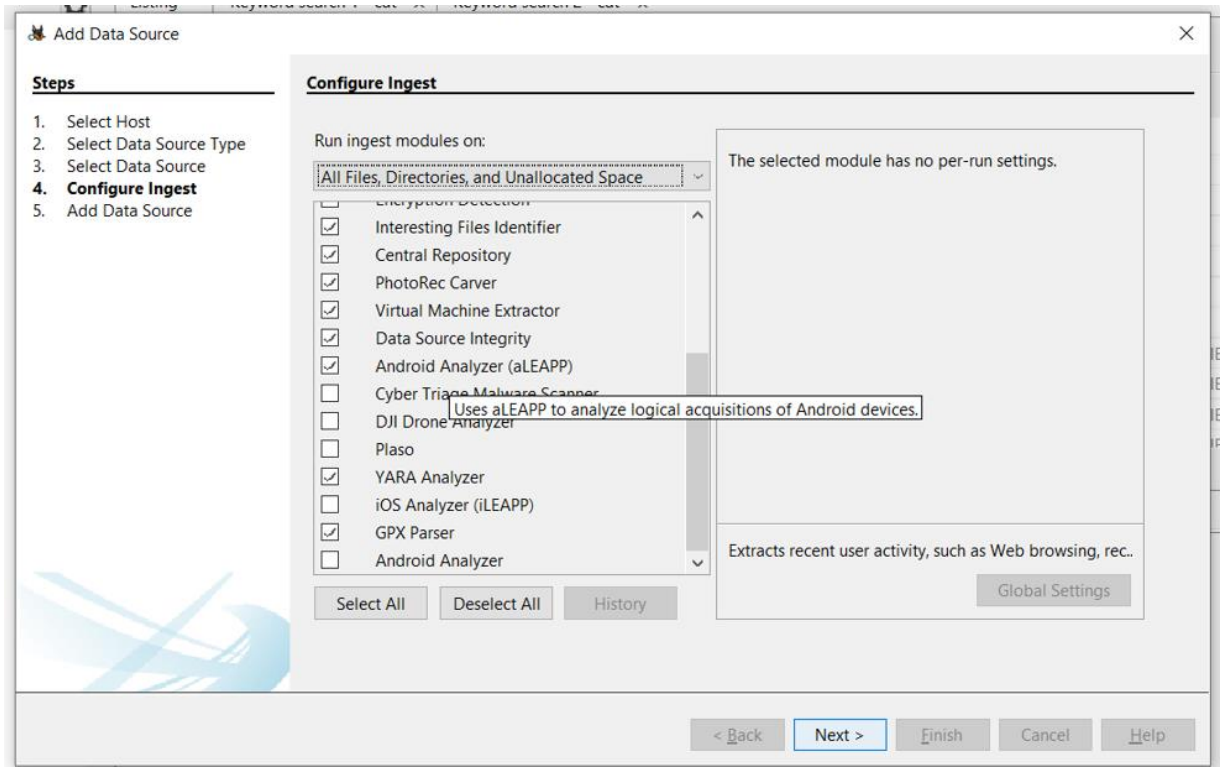


4. Setting path file dan waktu

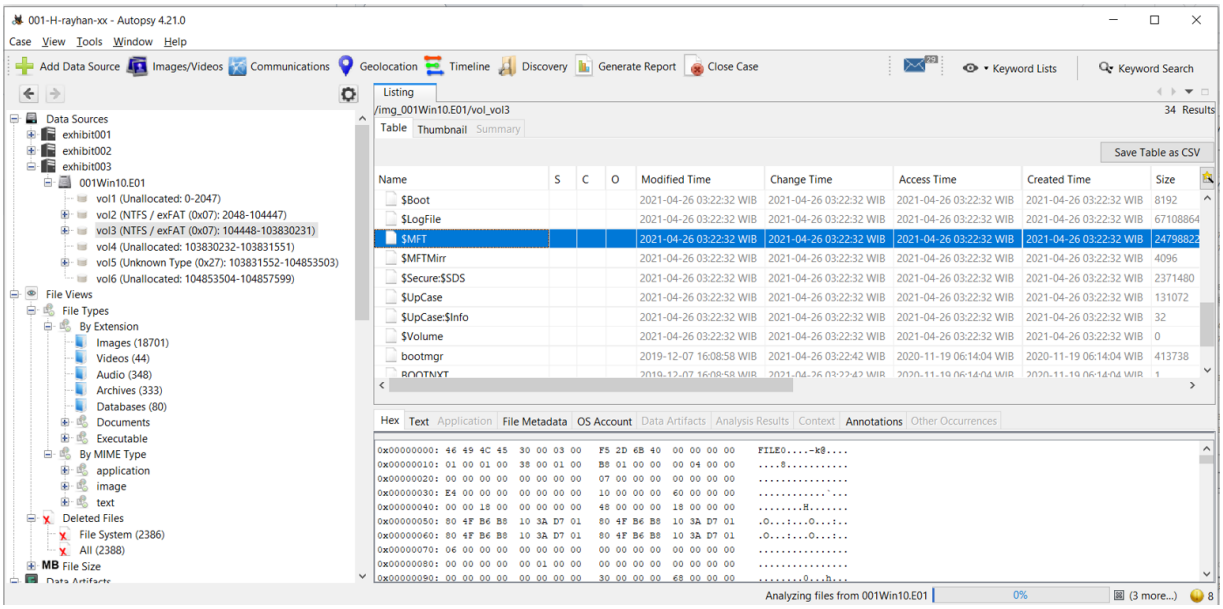


5. Centang kategori yang diperlukan

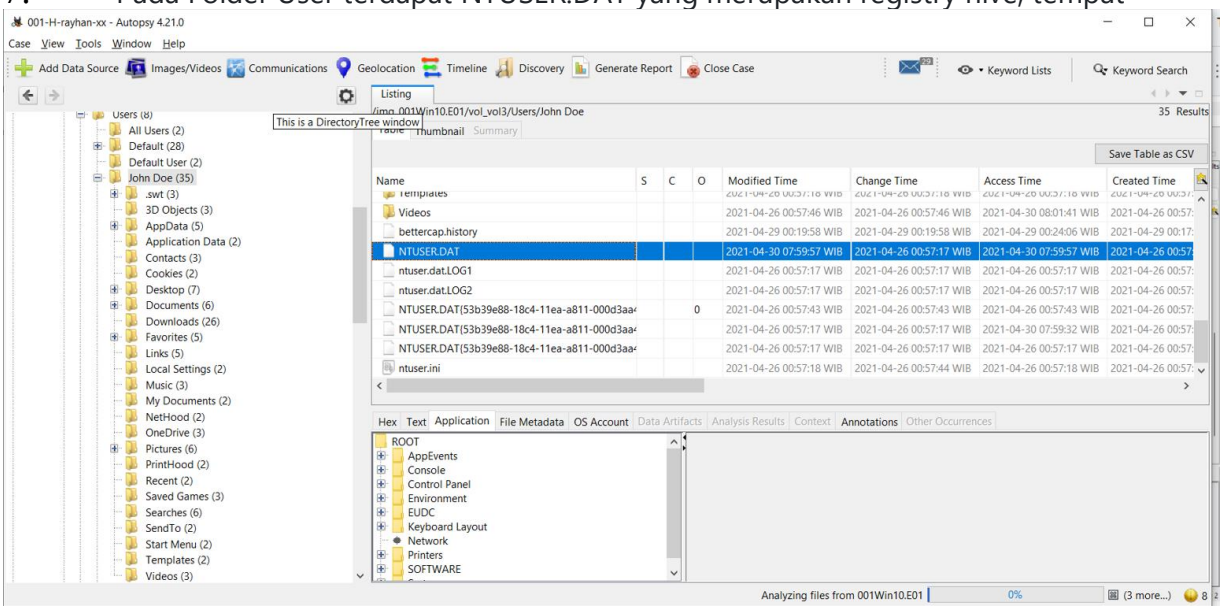




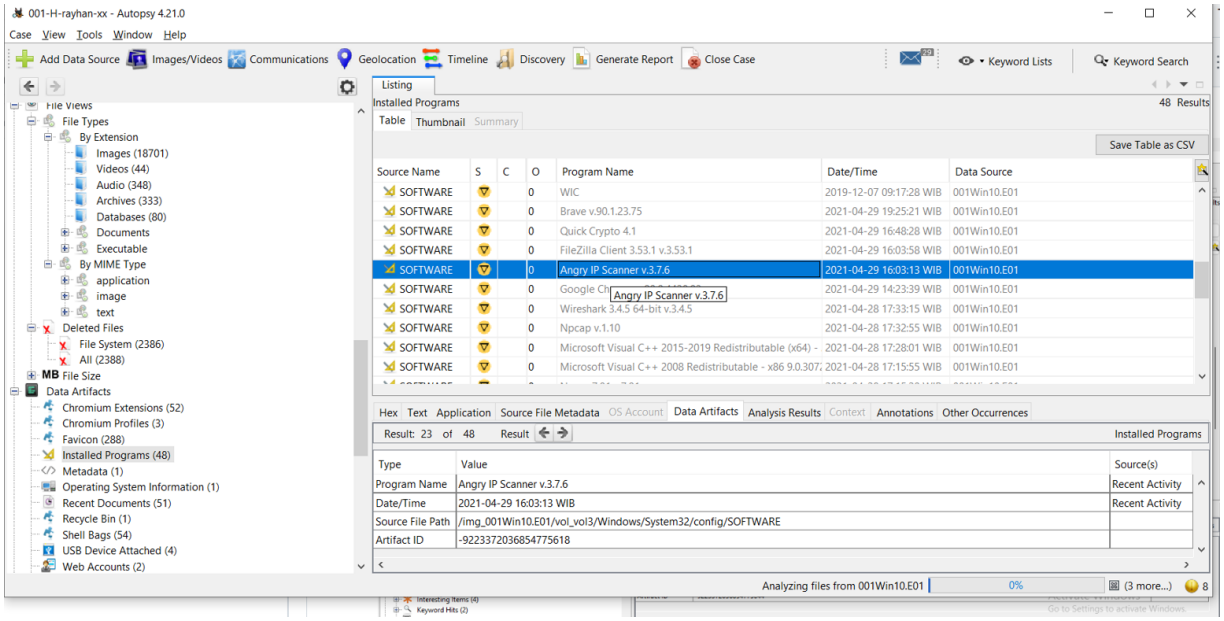
6. Pada Vol3 NTFS terdapat file $MFT yang berarti vol3 merupakan C drive.



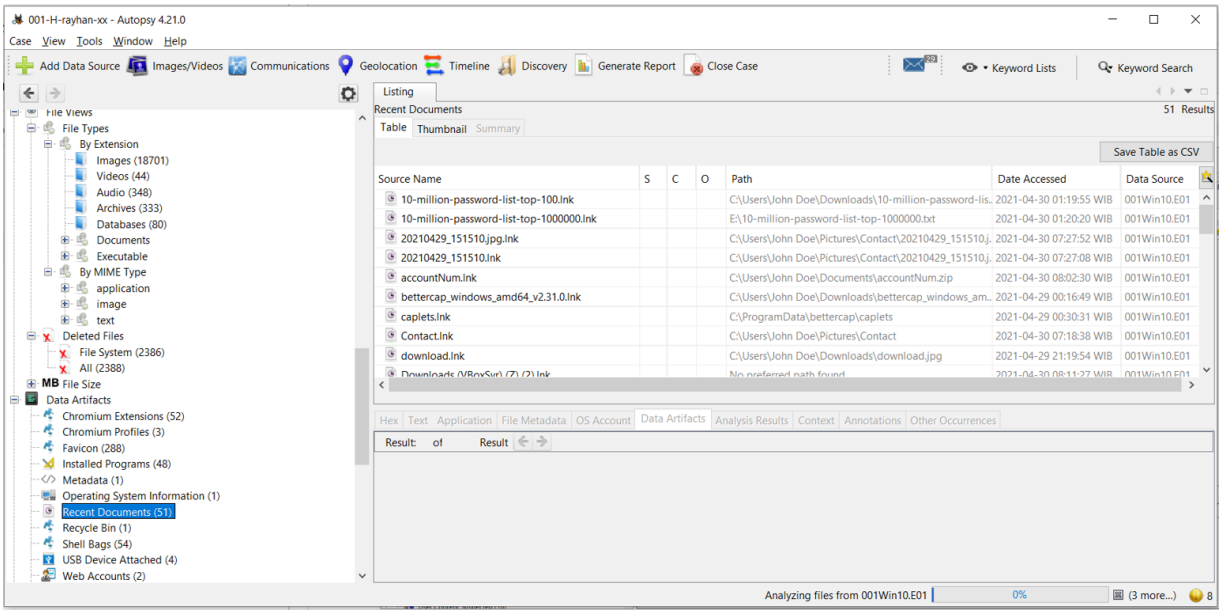
7. Pada Folder User terdapat NTUSER.DAT yang merupakan registry hive, tempat



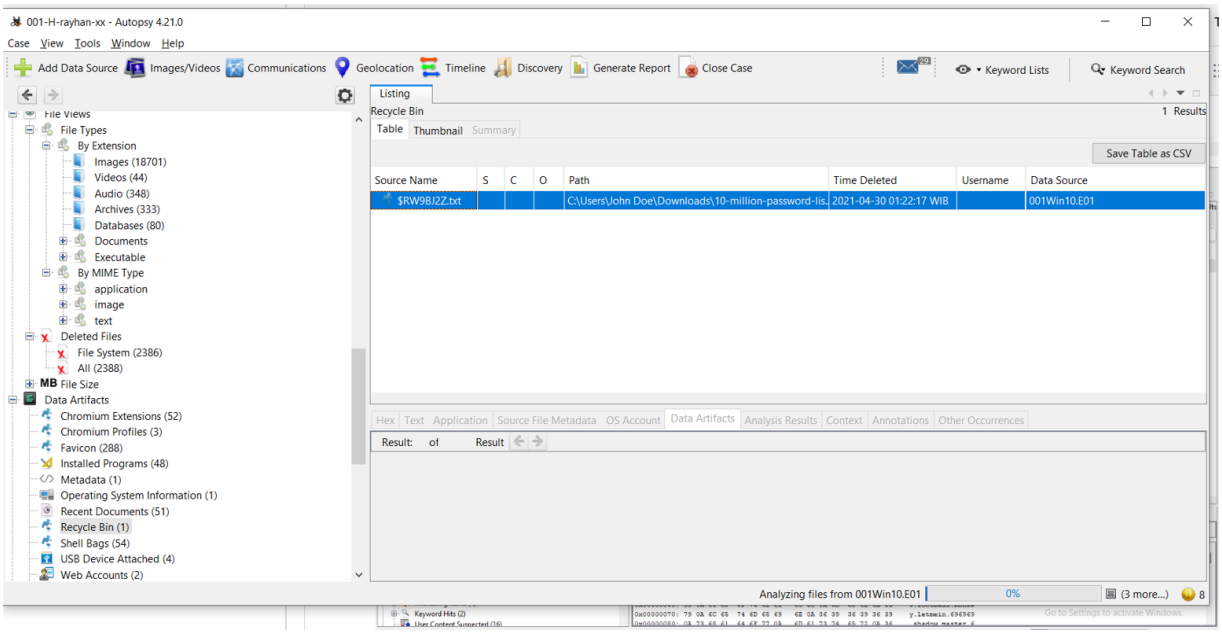
8. Pada Installed Programs di Data Artifact menampilkan informasi aplikasi apa saja yang telah di install di sistem



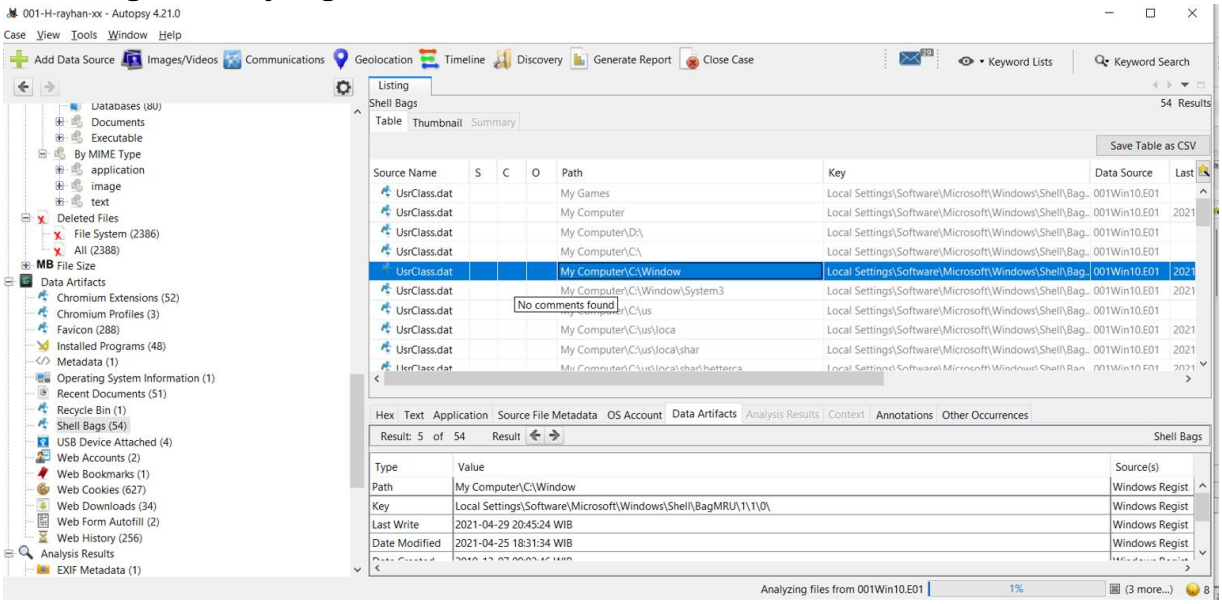
9. Recent document



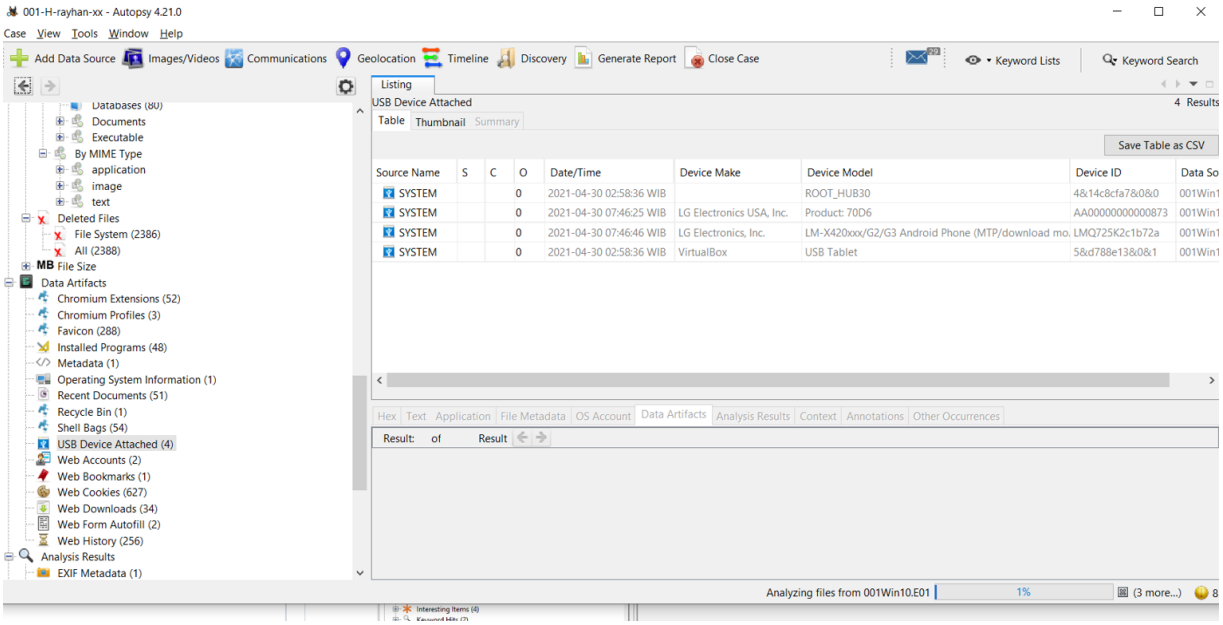
10. Reycle bin



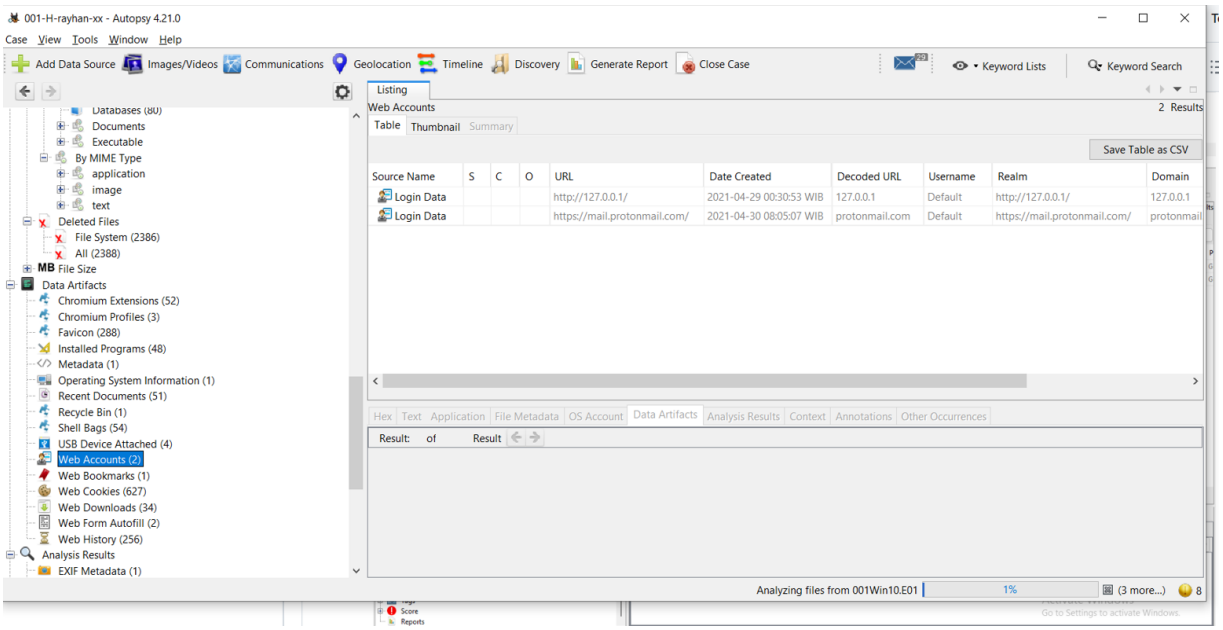
11. Shell bags folder yang diakses user



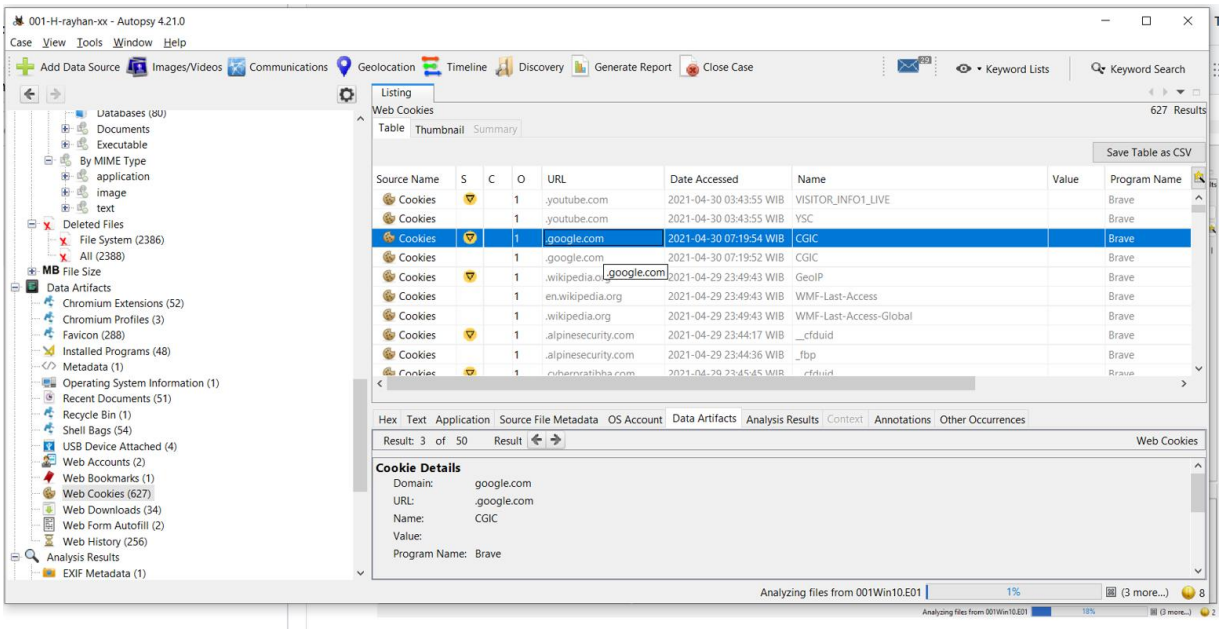
12. Usb deviced attached mengidentifikasi perangkat apa saja yang terconnect



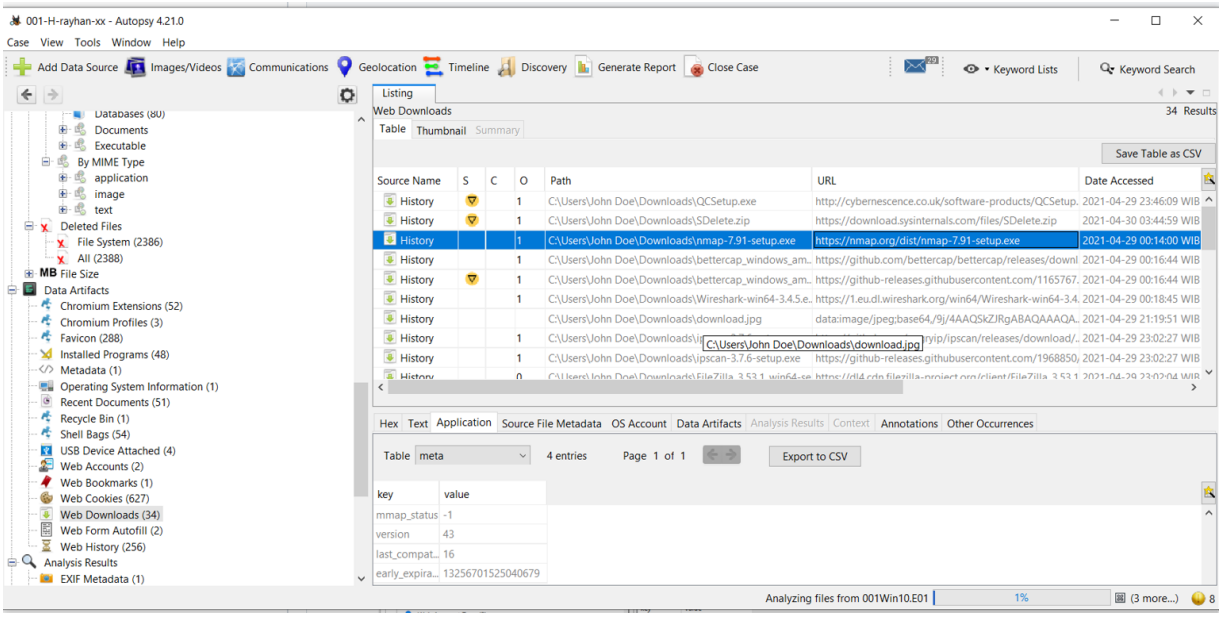
13. Web account tempat mengetahui kamu login dmana saja



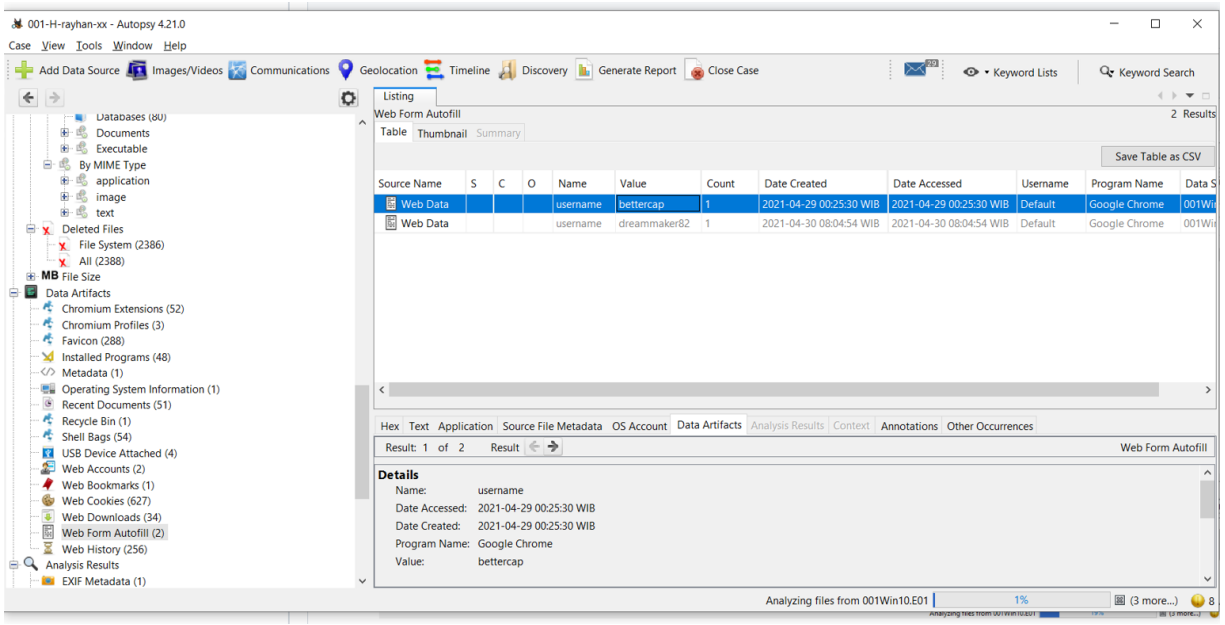
14. Web cookies berisi data tentang web yang pernah kamu masukin



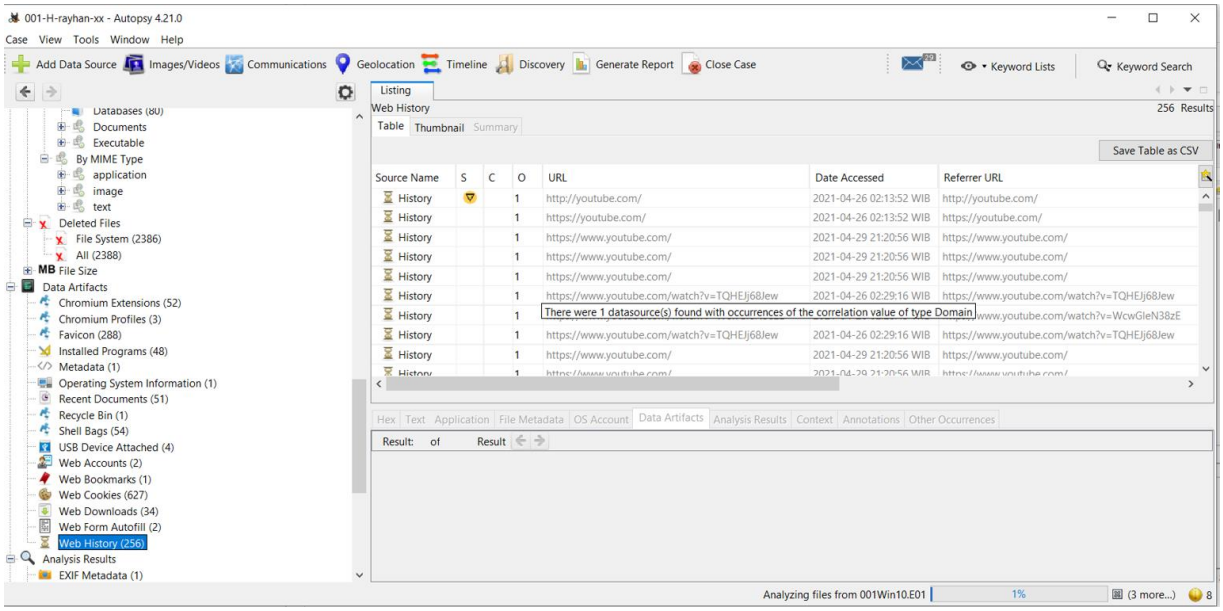
15. Web download berisi history download file yang berisi tgl dan tempat download.



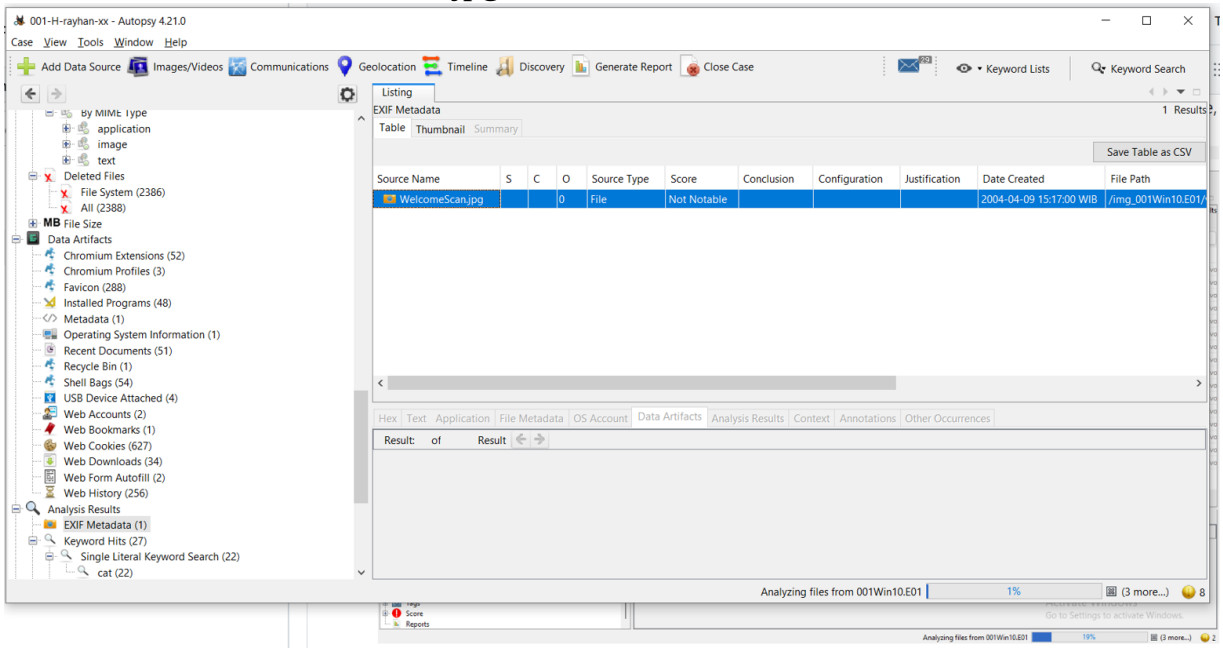
16. Web form autofill berisi data pengguna berupa username


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
Keyword Lists
Keyword Search
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
Web Data
username
bettercap
1
2021-04-29 00:25:30 WIB
2021-04-29 00:25:30 WIB
Default
Google Chrome
Web Data
username
dreammaker82
1
2021-04-30 08:04:54 WIB
2021-04-30 08:04:54 WIB
Default
Google Chrome
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
Databases (80)
Documents
Executable
By MIME Type
application
image
text
Deleted Files
File System (2386)
All (2388)
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)
Analyzing files from 001Win10.E01
1%
(3 more...)

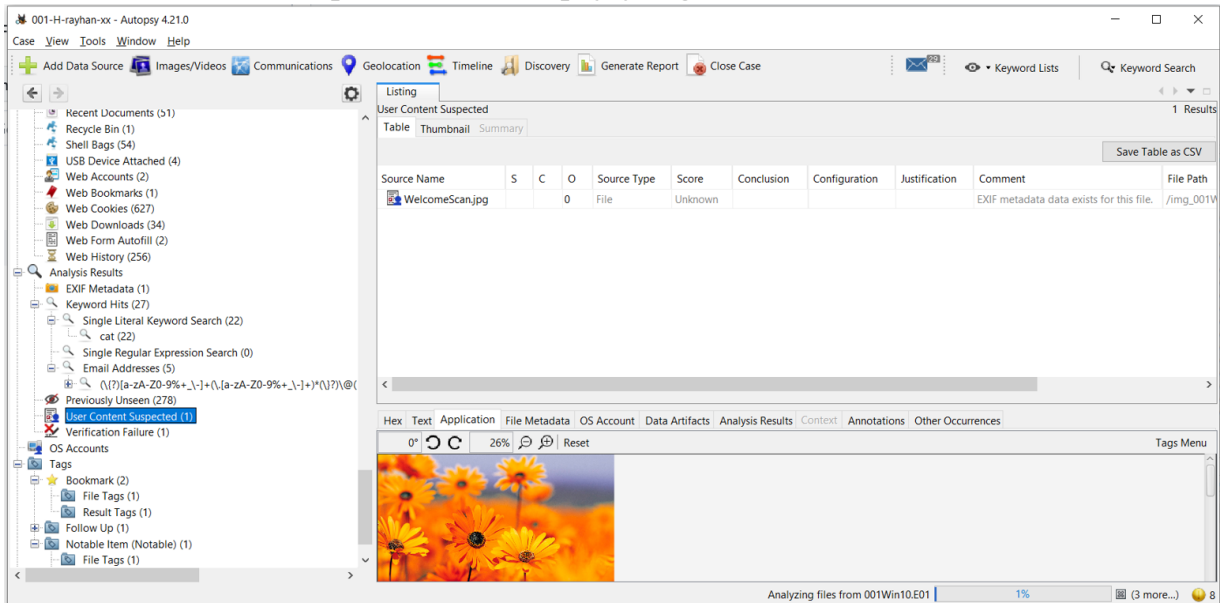
17. Web history berisi rekam jejak web pengguna



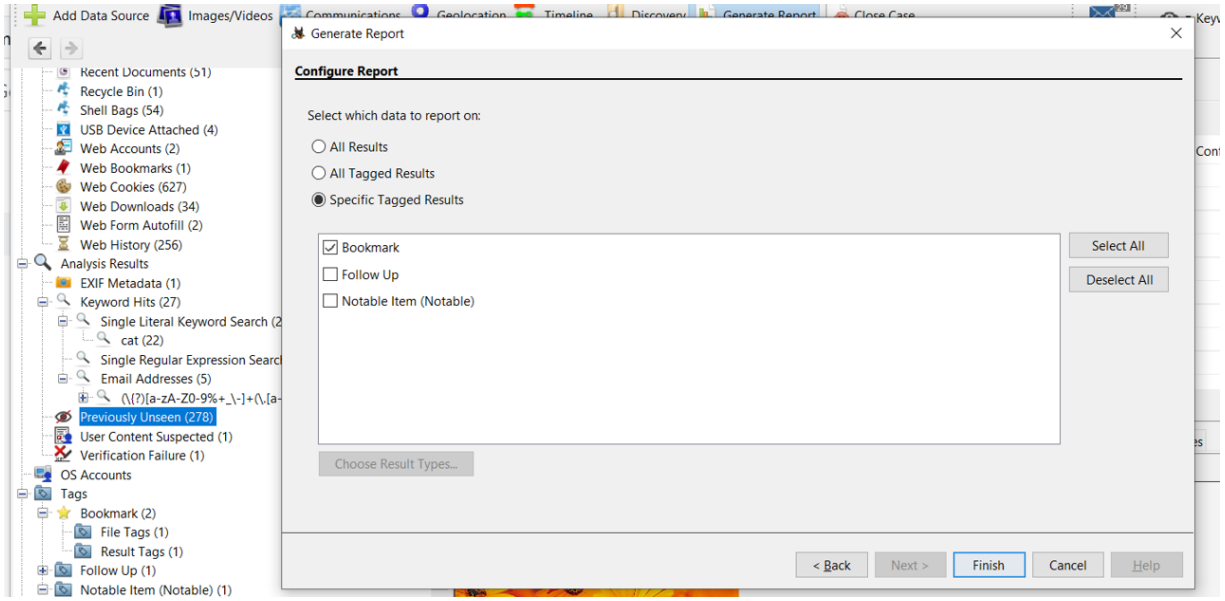
18. Exif metadata berisi file jpg



19. User content suspected file autopsy yang dibuat user



20. Generate report



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