
Mobile Forensic Fundamentals

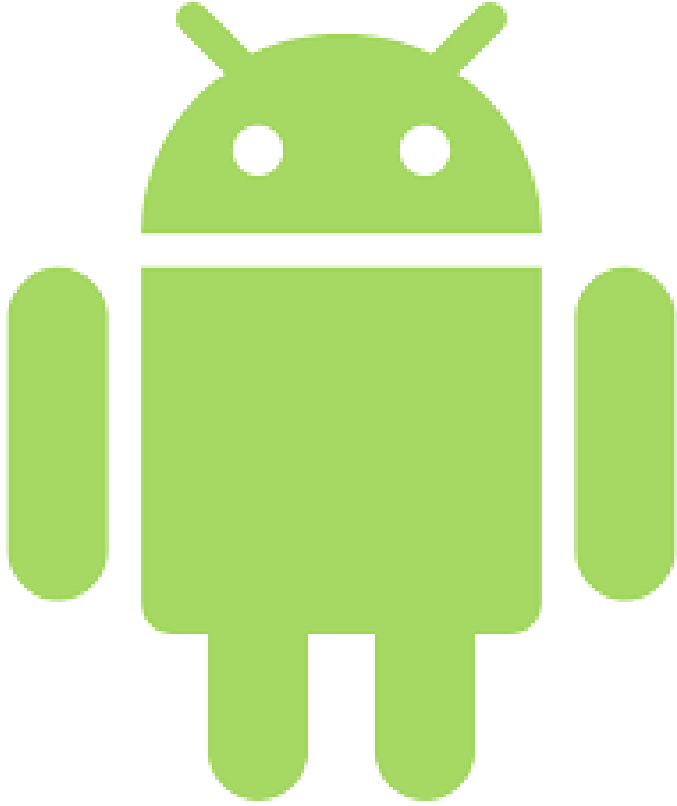
Android

Hacktrick, 2022

Irem Celik

İçerik

- Android Forensic Giriş
- Android Güvenlik Modeli
- Android Debug Bridge
- APK(Android Package Kit) Nedir?
- Android Cihazlarda Rootlama
- Android Dizin Yapısı
- İmaj Alma (Acquisition)
- Android Forensic Toolları
- Autopsy Dosya Analizi



Android Forensic Giriş

Android

71.59%

iOS

27.68%

Samsung

0.39%

Unknown

0.15%

KaiOS

0.12%

Nokia Unknown

0.02%

Mobile Operating System Market Share Worldwide - April 2022

Android Güvenlik Modeli

Application Sandboxing (Uygulama Koruma Alanı)

- Varsayılan olarak Android, Linux kullanıcı tabanlı koruma modelini kullanır.
- Atanan her android uygulaması benzersiz bir UID(unique identifier)'dir ve farklı bir işlem olarak çalıştırılır.
- Android'de, varsayılan olarak, bir uygulama başka bir uygulamanın verilerine erişemez. Bu nedenle, bir uygulama kötü amaçlı bir şey yapmaya çalışırsa, kendi bağlamı ve işletim sistemi tarafından atanan izin dahilinde yapabilir.(?)



Android Güvenlik Modeli

SELinux – Security Enhanced Linux
(Geliştirilmiş Güvenlik)

- Android 4.3 den itibaren desteklenmektedir.
- Uygulamanın yalıtılmış bir ortam da çalışmasını sağlayan MAC(Mandatory Access Control) kontrolünü kullanır.
- Bu şekilde zararlı bir yazılım kurulursa, işletim sistemine erişemez veya cihazı bozamaz.



Android Güvenlik Modeli

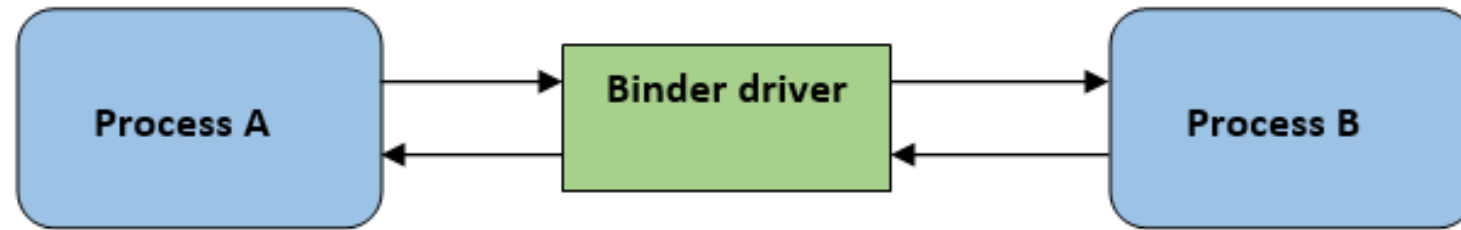
Application Signing (Uygulama imzalama)

- Android uygulamaları geliştirici sahibini belirlemek adına sahibi tarafından imzalanır.



Android Güvenlik Modeli

Secure Interprocess Communication



Android Güvenlik Modeli

User-based Permissions Model (Kullanıcı Tabanlı İzinler)

- Android default olarak linux çekirdeği üzerinde çalışır.
- Tüm istemci ve sunucu arasındaki iletişimin kontrolü linux çekirdeği tarafından yapılır.
- Android işletim sistemi her bir uygulama için izin modeli uygulamaktadır. Bu izinleri manifest.xml dosyasında tanımlar.
- Bu izinlerin tümü onaylandığı sürece uygulama kurulabilir.



Android Debug Bridge

- **A client:** Komutları bilgisayardan yazan kişi
- **A daemon :** Android cihazda komutları çalıştıran arka plan programı
- **A server :** Client ve Daemon arasındaki iletişimi sağlayan bilgisayardaki arka plan süreci
- **adb shell :** Android cihaz ile bağlantı kurmamızı sağlayan terminal



APK (Android Package Kit) Nedir?

- META-INF/
- lib/
- res/
- assets/
- AndroidManifest.xml
- classes.dex
- resources.arsc



Android Cihazlarda Rootlama

- Uygun bir Linux sisteminde yapabileceğiniz hemen hemen her şeyi, telefonunuzda root erişimi ile yapabilirsiniz.
- Sistem uygulamalarını kaldırabilir,yüklü uygulamaların gerektirdiği izinleri iptal edebilir.



Android Dizin Yapısı

- /system
- /data
- /sdcard

```
root@generic:/ # ls -l
drwxr-xr-x root    root          2016-02-18 08:23 acct
drwxrwx--- system  cache        2016-02-18 07:01 cache
dr-x----- root    root          2016-02-18 08:23 config
lrwxrwxrwx root    root          2016-02-18 08:23 d -> /sys/kernel/debug
drwxrwx--x system  system       2016-02-18 07:01 data
-rw-r--r-- root    root          116 1969-12-31 19:00 default.prop
drwxr-xr-x root    root          2016-02-18 08:23 dev
lrwxrwxrwx root    root          2016-02-18 08:23 etc -> /system/etc
-rw-r--r-- root    root          8870 1969-12-31 19:00 file_contexts
-rw-r----- root    root          953 1969-12-31 19:00 fstab.goldfish
-rwxr-x--- root    root        175260 1969-12-31 19:00 init
-rwxr-x--- root    root          919 1969-12-31 19:00 init.environ.rc
-rwxr-x--- root    root          2979 1969-12-31 19:00 init.goldfish.rc
-rwxr-x--- root    root        20177 1969-12-31 19:00 init.rc
-rwxr-x--- root    root          1795 1969-12-31 19:00 init.trace.rc
-rwxr-x--- root    root          3915 1969-12-31 19:00 init.usb.rc
drwxrwxr-x root    system       2016-02-18 08:23 mnt
dr-xr-xr-x root    root          1969-12-31 19:00 proc
-rw-r--r-- root    root          2161 1969-12-31 19:00 property_contexts
drwx----- root    root          2013-07-09 20:46 root
drwxr-x--- root    root          1969-12-31 19:00 sbin
lrwxrwxrwx root    root          2016-02-18 08:23 sdcard -> /storage/sdcard
-rw-r--r-- root    root          656 1969-12-31 19:00 seapp_contexts
-rw-r--r-- root    root        74816 1969-12-31 19:00 sepolicy
drwxr-x--x root    sdcard_r     2016-02-18 08:23 storage
dr-xr-xr-x root    root          2016-02-18 08:22 sys
drwxr-xr-x root    root          1969-12-31 19:00 system
-rw-r--r-- root    root          272 1969-12-31 19:00 ueventd.goldfish.rc
-rw-r--r-- root    root          4024 1969-12-31 19:00 ueventd.rc
lrwxrwxrwx root    root          2016-02-18 08:23 vendor -> /system/vendor
root@generic:/ #
```

/system

```
root@generic:/ # cd system/  
root@generic:/system # ls -l  
drwxr-xr-x root    root          2015-02-18 21:31 app  
drwxr-xr-x root    shell         2015-02-18 21:27 bin  
-rw-r--r-- root    root          1507 2015-02-18 21:20 build.prop  
drwxr-xr-x root    root          2015-02-18 21:36 etc  
drwxr-xr-x root    root          2015-02-18 21:24 fonts  
drwxr-xr-x root    root          2015-02-18 21:29 framework  
drwxr-xr-x root    root          2015-02-18 21:29 lib  
drwx----- root    root          1969-12-31 19:00 lost+found  
drwxr-xr-x root    root          2015-02-18 21:23 media  
drwxr-xr-x root    root          2015-02-18 21:31 priv-app  
drwxr-xr-x root    root          2015-02-18 21:23 tts  
drwxr-xr-x root    root          2015-02-18 21:23 usr  
drwxr-xr-x root    shell        2015-02-18 21:27 xbin  
root@generic:/system # █
```

/data

- /data/app: apk dosyaları

```
root@generic:/ # cd /data/app
root@generic:/data/app # ls
ApiDemos.apk
ApiDemos.odex
CubeLiveWallpapers.apk
CubeLiveWallpapers.odex
GestureBuilder.apk
GestureBuilder.odex
SmokeTest.apk
SmokeTest.odex
SmokeTestApp.apk
SmokeTestApp.odex
SoftKeyboard.apk
SoftKeyboard.odex
WidgetPreview.apk
WidgetPreview.odex
root@generic:/data/app # █
```

/data/data

```
root@generic:/data/data/com.android.browser # ls -l
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 app_appcache
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 app_databases
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 app_geolocation
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 app_icons
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:34 app_webview
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 cache
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 databases
lrwxrwxrwx install  install   2016-02-18 06:59 lib -> /data/app-lib/com.android.browser
drwxrwx--x u0_a14    u0_a14    2016-02-18 08:33 shared_prefs
root@generic:/data/data/com.android.browser # █
```

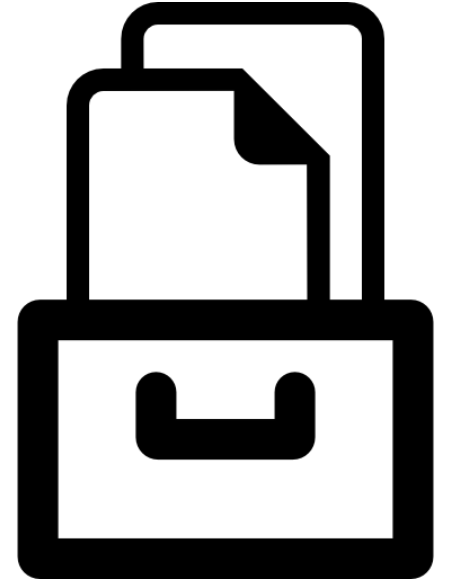
/data/data/com.android.browser

/data/data/<Uygulama Paket İsmi>/

Dosya İsmi	Açıklama
lib	Uygulamanın gerektirdiği kütüphane dosyaları
files	Geliştiricinin kaydettiği dosyalar
cache	Uygulama tarafından önbelleğe alınan dosyalar
databases	SQLite veritabanları ve günlük dosyaları
shared_prefs	Paylaşılan tercihlerin XML'si

İmaj Alma (Acquisition)

- **Fiziksel:** Mobil cihazın tamamının birebir imajının alınmasıyla gerçekleştirilir, silinen veriler de geri getirilir. En iyi delil olarak nitelendirilir.
- **Mantıksal:** Dosya ve klasör sisteminin mantıksal kopyasıdır.
- **Manual:** İncelemeyi gerçekleştiren uzmanın, mobil cihaza ait tuş takımı veya dokunmatik ekranı kullanarak, cihazın işletim sistemi arayüzü ve menülerinde gezinip elde ettiği dijital delillerin ekran görüntülerini alması yoluyla gerçekleştirdiği veri elde etme yöntemidir. İnsan faktörü ve dijital delillerin silinmesi gibi ihtimaller göz önünde bulundurulduğunda, bu veri elde etme yönteminin oldukça riskli olduğu belirtilmektedir .



Android Forensic Toolları

The logo for LIME (Linux Memory Extractor) features the word "LIME" in a large, bold, yellow-green font. The background of the logo is a dark, blurred image of a server room with multiple computer monitors displaying code.

LIME

Linux Memory Extractor



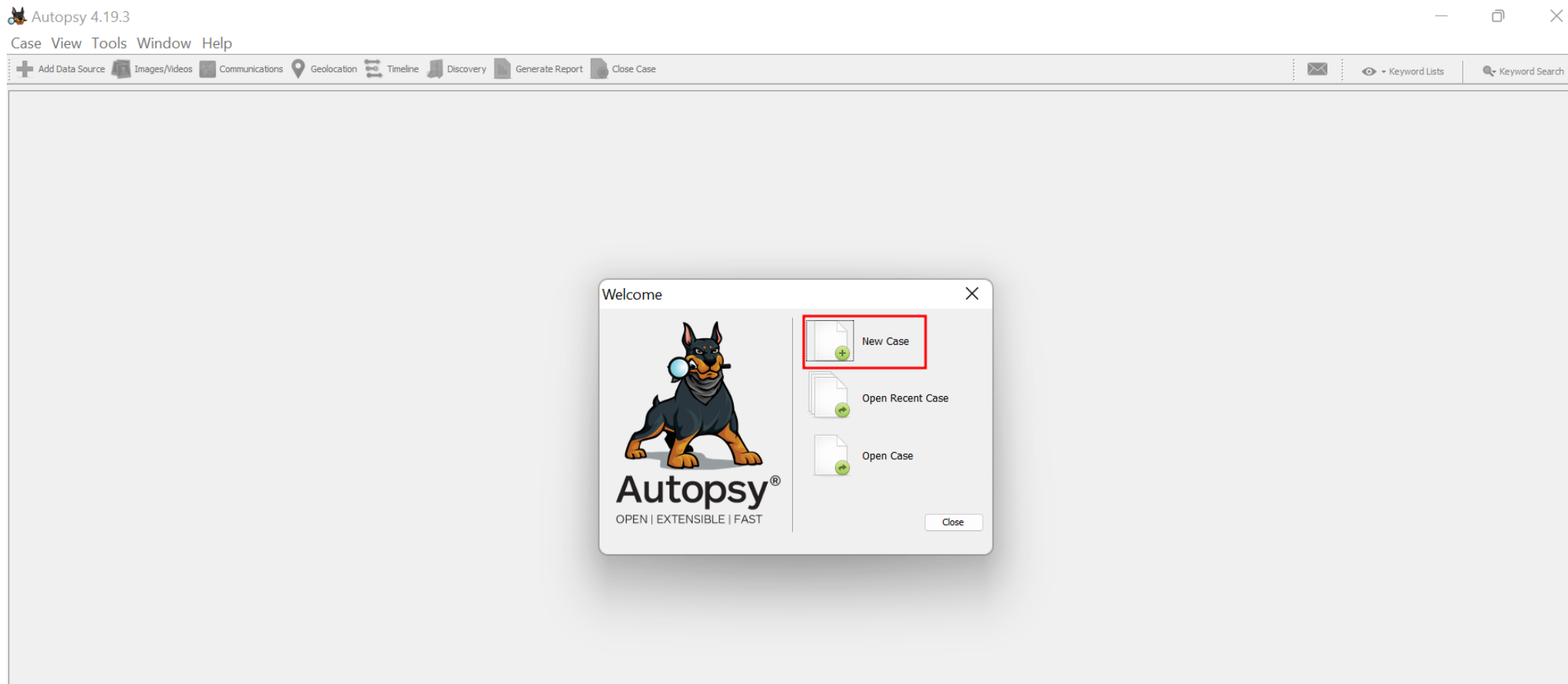
Autopsy

DIGITAL FORENSIC TOOL

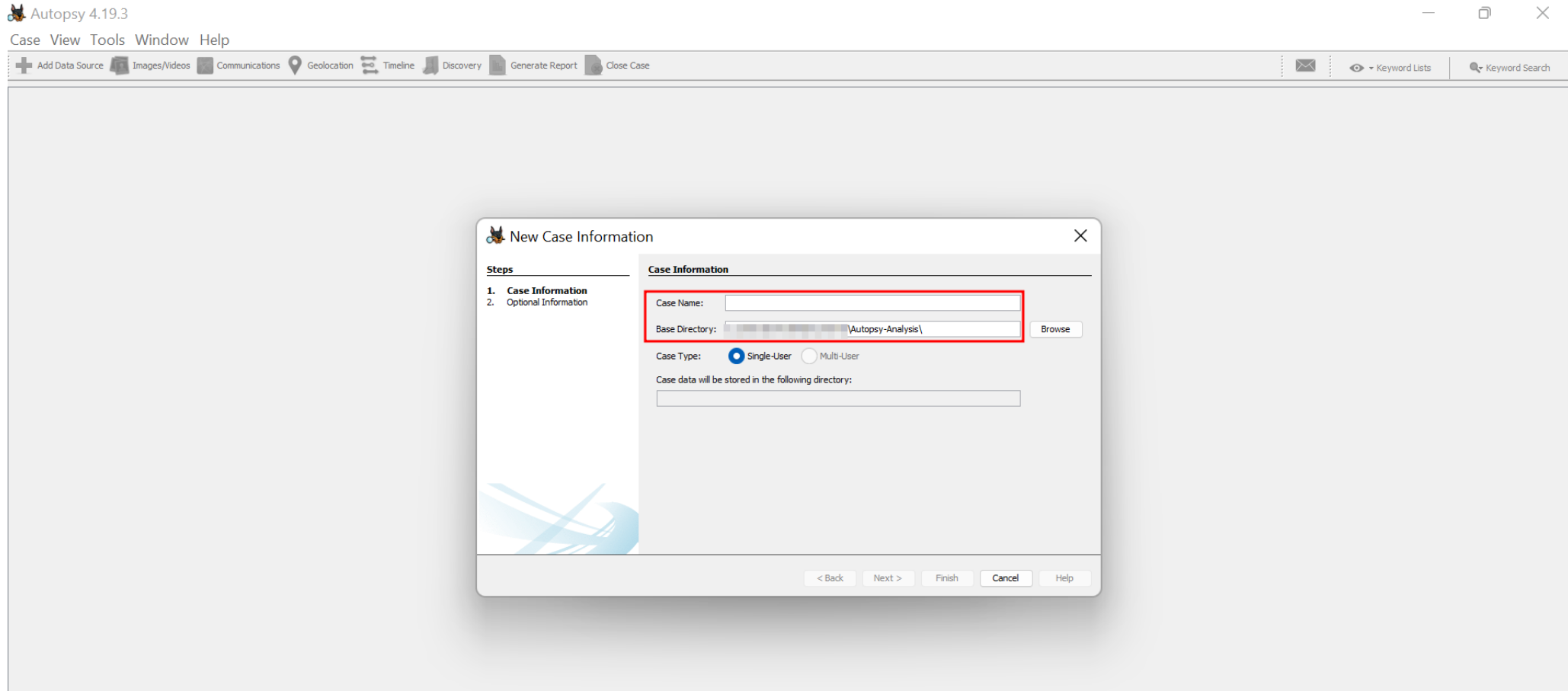


ANDROID DATA EXTRACTOR LITE

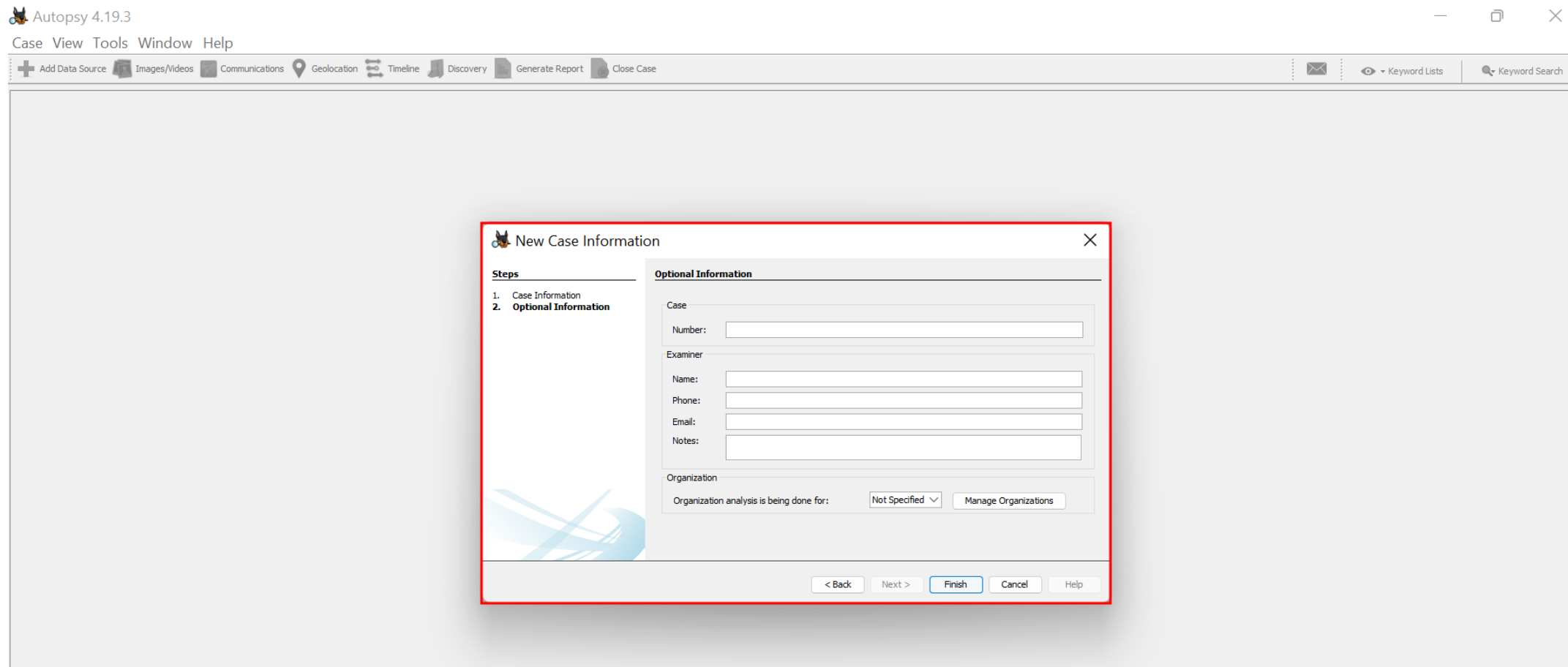
Autopsy Dosya Analizi



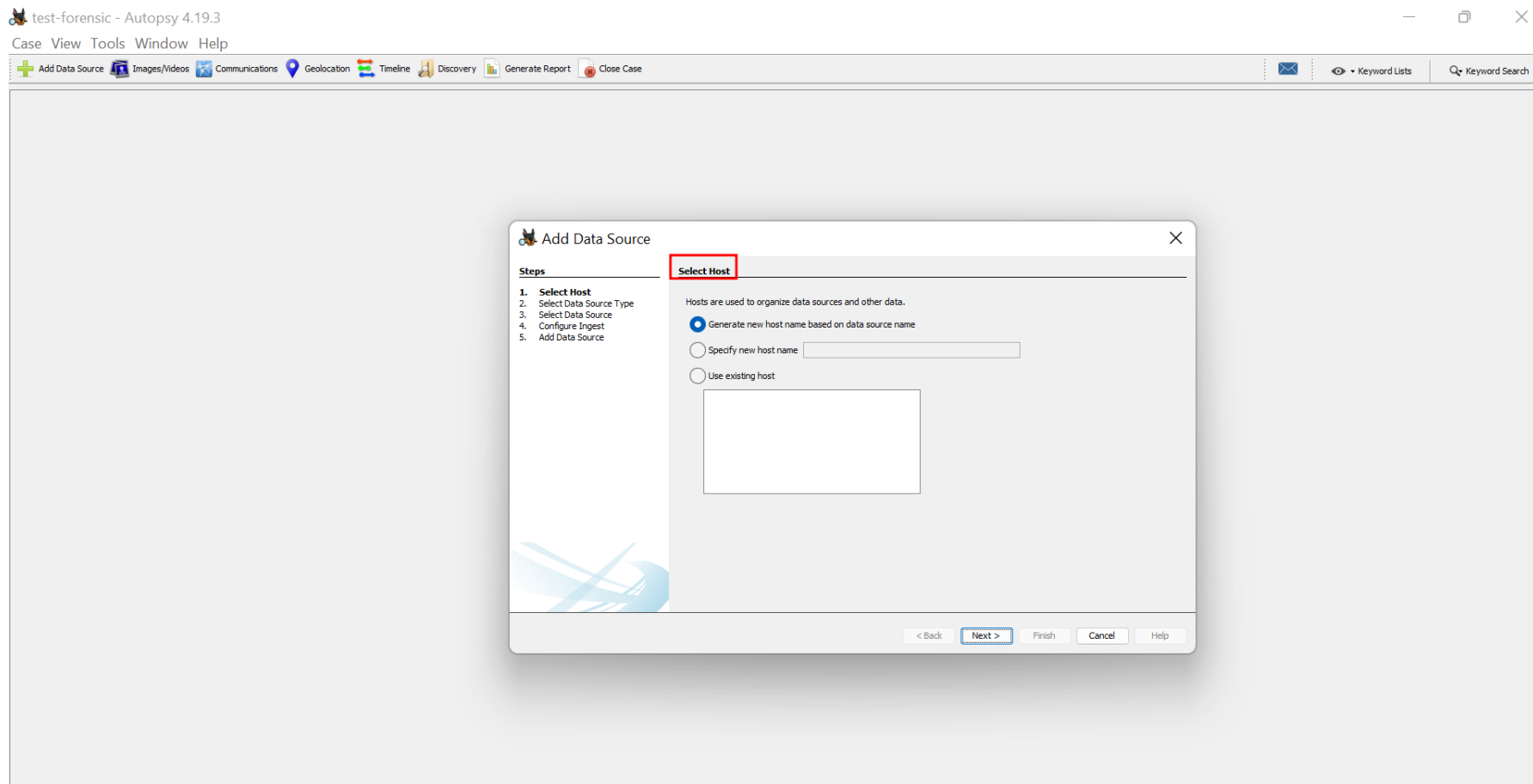
Autopsy Dosya Analizi



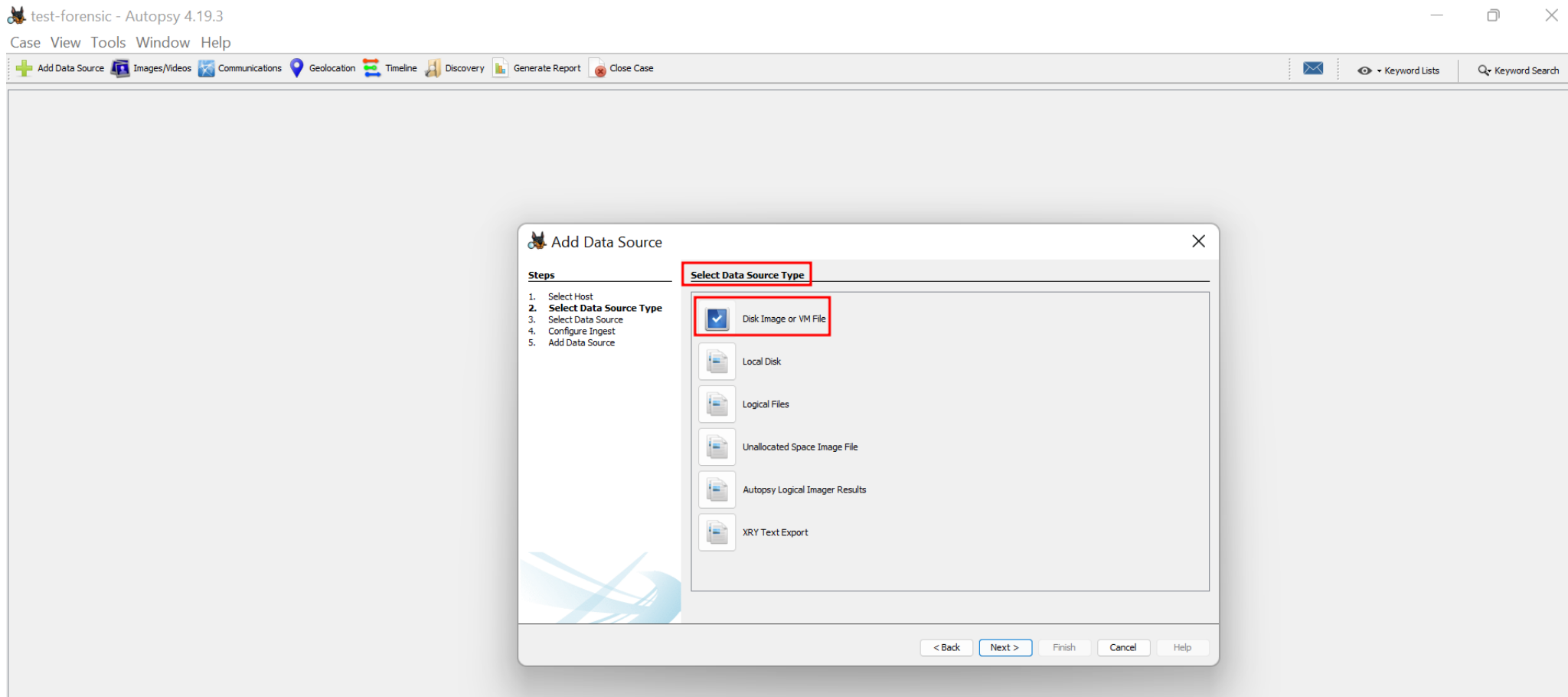
Autopsy Dosya Analizi



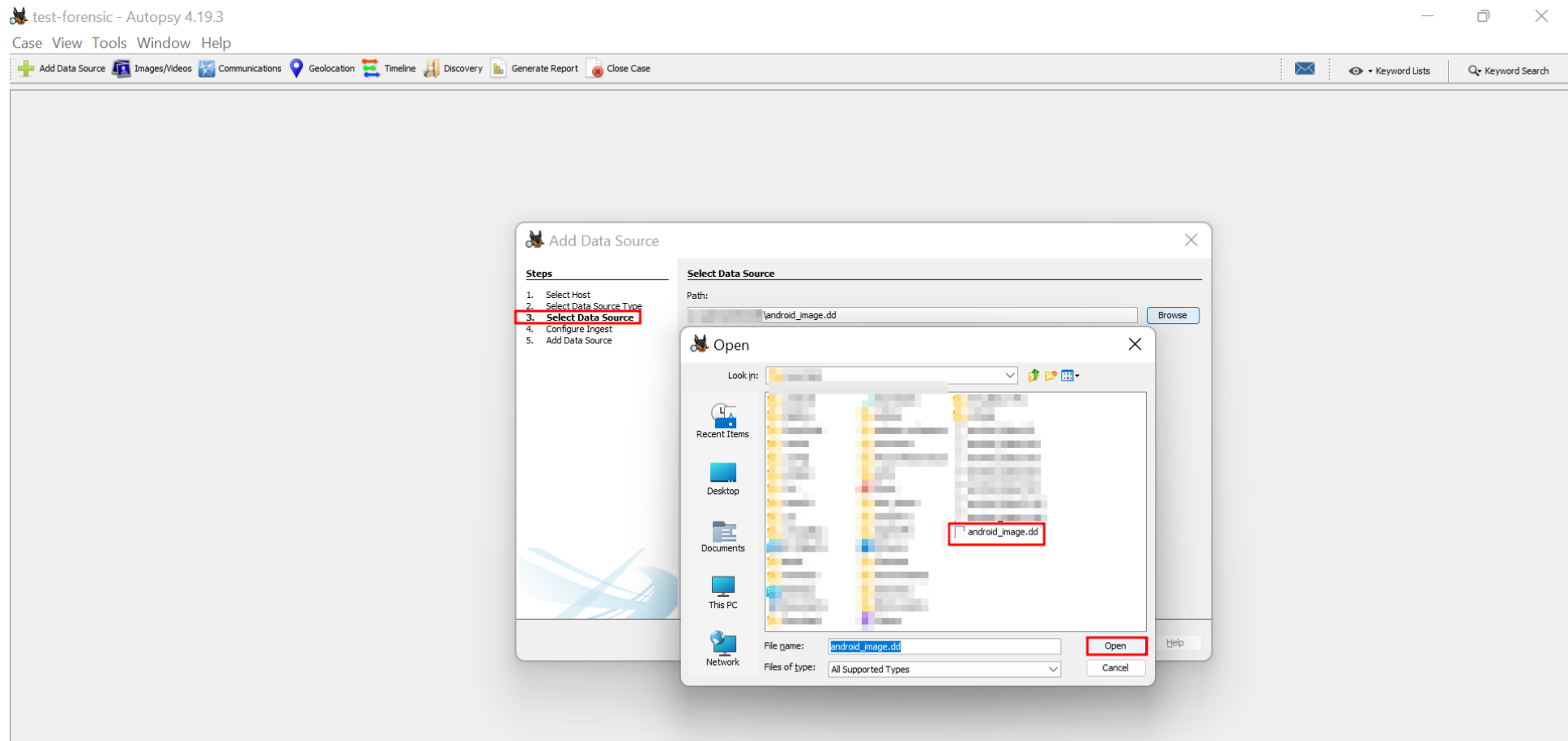
Autopsy Dosya Analizi



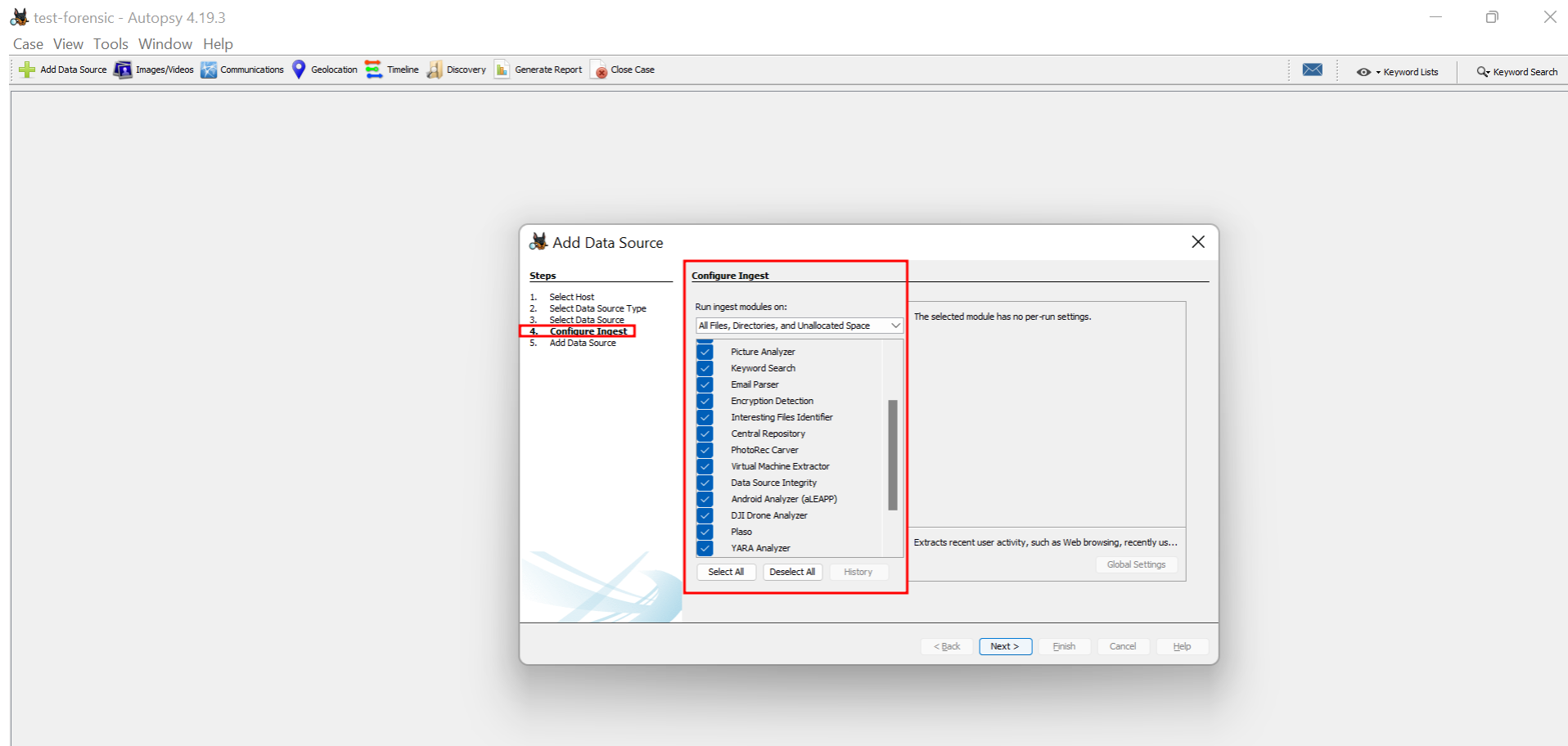
Autopsy Dosya Analizi



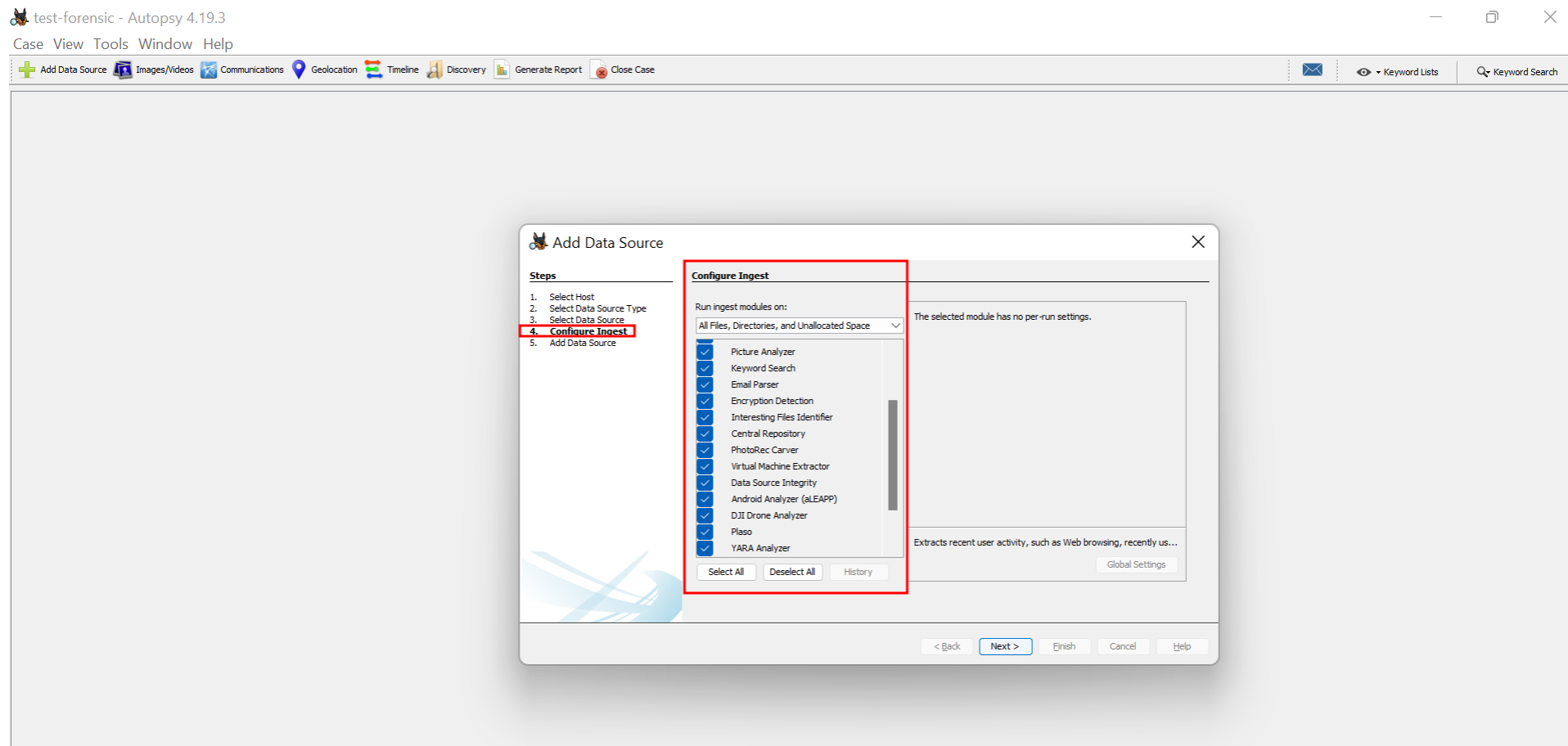
Autopsy Dosya Analizi



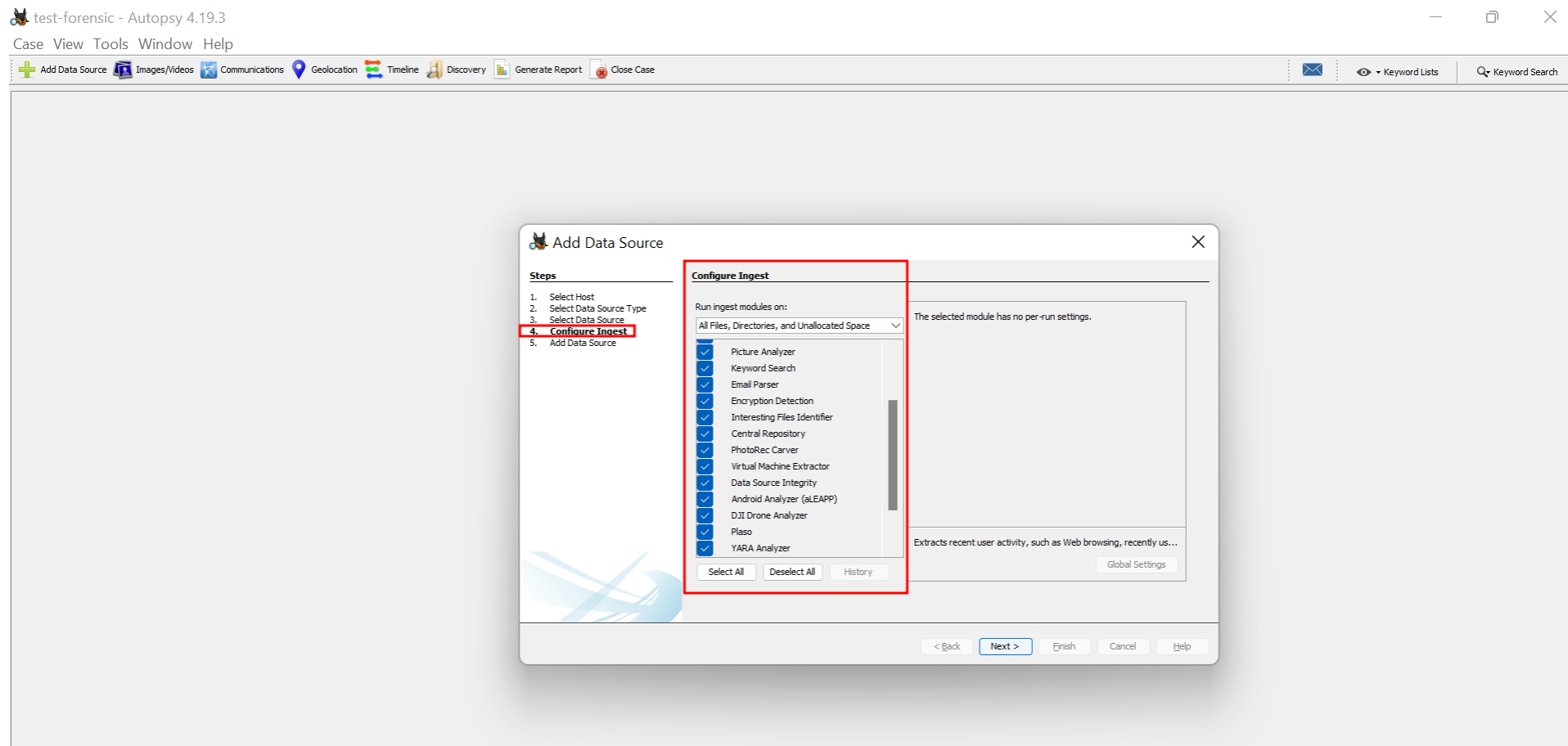
Autopsy Dosya Analizi



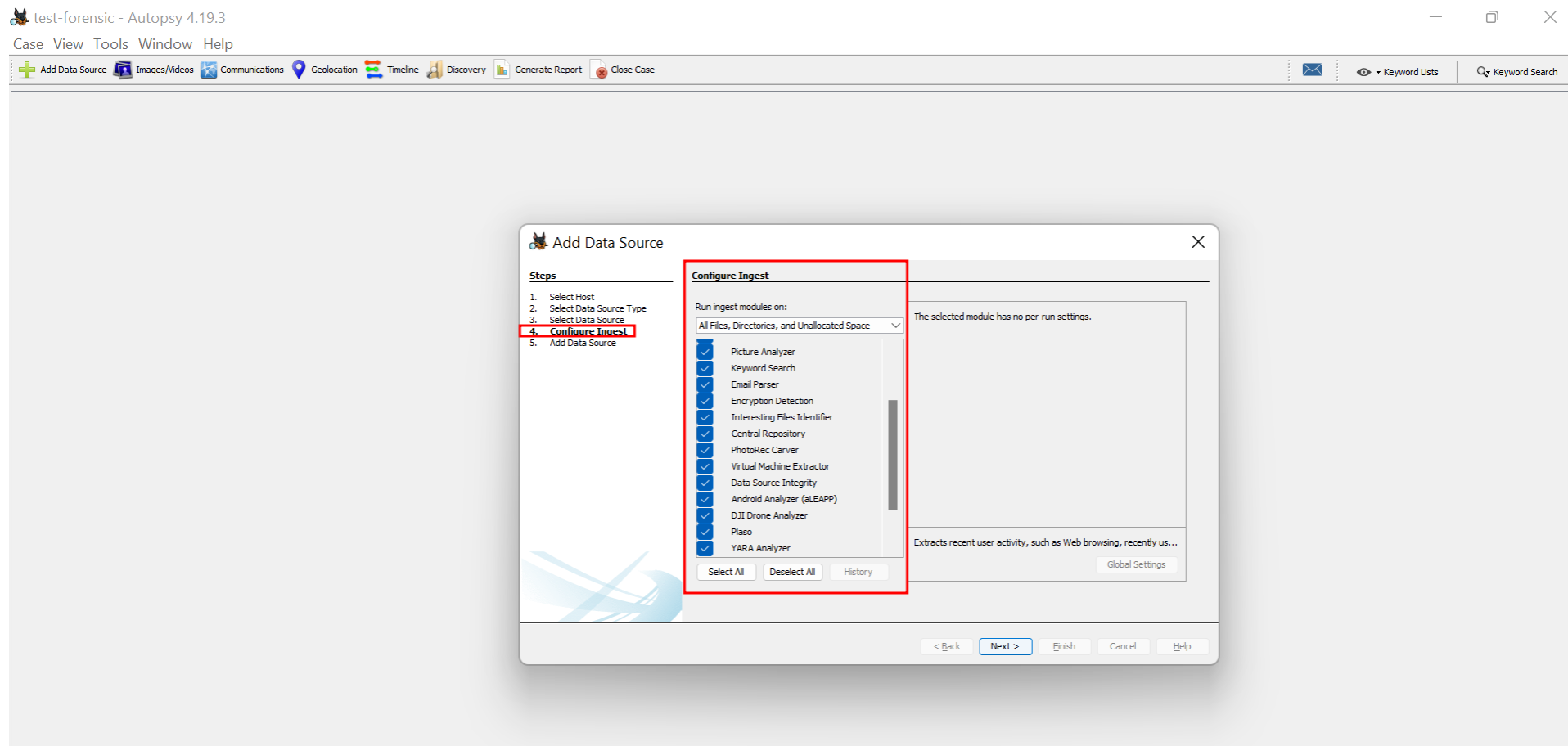
Autopsy Dosya Analizi



Autopsy Dosya Analizi



Autopsy Dosya Analizi



Autopsy Dosya Analizi

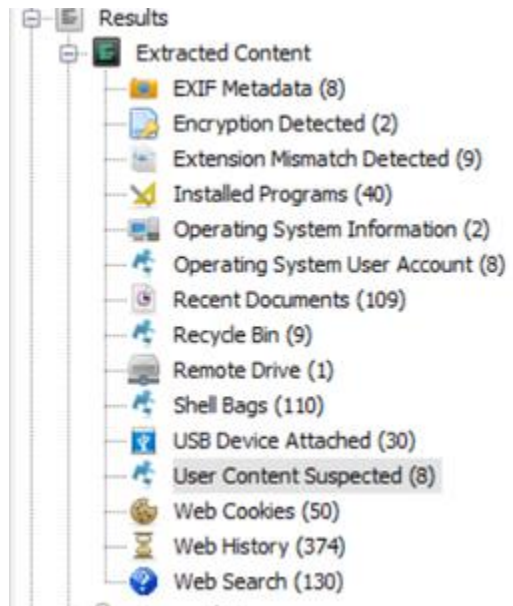
The screenshot displays the Autopsy software interface. The main window shows a file system listing with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). A context menu is open over a selected row, with 'Extract File(s)' highlighted. The left sidebar shows a tree view of data sources and results. The bottom pane shows file properties for the selected file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Key
nb-NO			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
zh-TW			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
connection			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
tool			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
System			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
System			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
FD9			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
Jetio			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
Micro			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
Spide			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur
xi ST			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		ur

File Properties for: /vol_vol2/Program Files/AIM6/services/connection

Name	File System
Type	application/octet-stream
MIME Type	application/octet-stream
Size	0
File Name Allocation	Unallocated
Metadata Allocation	
Modified	0000-00-00 00:00:00
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
MD5	d41d8cd98f00b204e9800998ecf8427e
Hash Lookup Results	UNKNOWN

Autopsy Dosya Analizi



Autopsy Dosya Analizi

The screenshot displays the Autopsy software interface. The top menu bar includes 'Case', 'View', 'Tools', 'Window', and 'Help'. Below the menu is a toolbar with icons for 'Add Data Source', 'Images/Videos', 'Communications', 'Geolocation', 'Timeline', 'File Discovery', 'Generate Report', and 'Close Case'. The main window is divided into several panes:

- Data Sources:** A tree view on the left showing the file system structure, including 'Mantooth.E01' and various volumes (vol1, vol2, vol3, vol4).
- Listing:** A table view showing a list of files. The selected file is an Outlook PST file.
- Message:** A preview of the selected email message, showing the 'From', 'To', 'Subject', and 'Text' tabs.

Source File	S	C	O	E-Mail To	Subject	Message ID	Path	Thread ID
Outlook.pst				'Rasco Badguy'	Read: Letter	2098500	\	0cc2850e-e56f
Outlook.pst				dollarhyde86@comcast.net	Microsoft Office Outlook Test Message	2097220	\\Top of Personal Folders\Deleted Items	23afa8b0-692d
Outlook.pst				New Outlook User	Welcome to Microsoft Office Outlook 2003	2097188	\\Top of Personal Folders\Deleted Items	55ee6424-fe2f
Outlook.pst				Mantooth	Whats up in D town?	2097252	\\Top of Personal Folders\Inbox	1ae1b9f8-2dfc
Outlook.pst				Wes Mantooth	Re: Whats up in D town?	2097316	\\Top of Personal Folders\Inbox	1ae1b9f8-2dfc
Outlook.pst				Wes Mantooth	Re: Whats up in D town?	2097380	\\Top of Personal Folders\Inbox	1ae1b9f8-2dfc
Outlook.pst				chkwasher@comcast.net; dollarhyde86@comcast.net; mol...	Letter	2098468	\\Top of Personal Folders\Inbox	0cc2850e-e56f
Outlook.pst				'John Washer'	RE: Whats up in D town?	2097284	\\Top of Personal Folders\Sent Items	1ae1b9f8-2dfc

The email message preview shows the following details:

- From:** dollarhyde86@comcast.net: dollarhyde86@comcast.net
- To:** dollarhyde86@comcast.net
- Subject:** Microsoft Office Outlook Test Message
- Text:** This is an e-mail message sent automatically by Microsoft Office Outlook's Account Manager while testing the settings for your POP3 account.

Autopsy Dosya Analizi

The screenshot displays the Autopsy software interface during a report generation process. The main window shows a file listing with columns for Source Module Name, Report Name, Created Time, and Report File Path. A dialog box titled "Generate Report" is open, allowing the user to "Select and Configure Report Modules".

Generate Report Dialog - Report Modules:

- HTML Report
- Excel Report
- Files - Text
- Save Tagged Hashes
- TSK Body File
- Google Earth KML
- STIX
- CASE-UCO
- Portable Case

The dialog also includes a description: "A report about results and tagged items in Excel (XLS) format." and a note: "This report will be configured on the next screen." Buttons for "< Back", "Next >", "Finish", "Cancel", and "Help" are visible at the bottom of the dialog.

The background interface shows a file listing with 7 results. The hex view at the bottom displays data in hexadecimal and ASCII format, including file paths like "user's Adobe Rea" and "Adobe Acrobat Rea".

Thank you!
Any Questions?



www.prplbx.com