PurpleBox

Mobile Forensic Fundamentals

Android

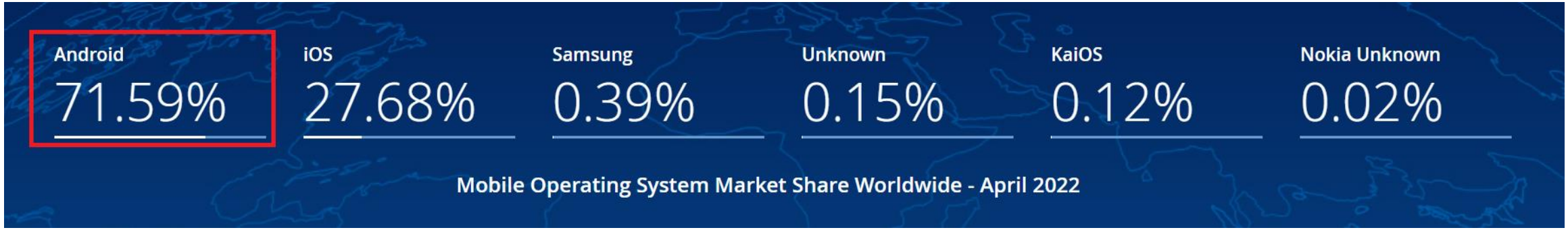
Hacktrick, 2022

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(Mendotory Access Control) kontrolünü kullanır.
- Bu şekilde zararlı bir yazılım kurulursa, işletim sistemine erişemez veya cihazı bozamaz.

Android Güvenlik Modeli

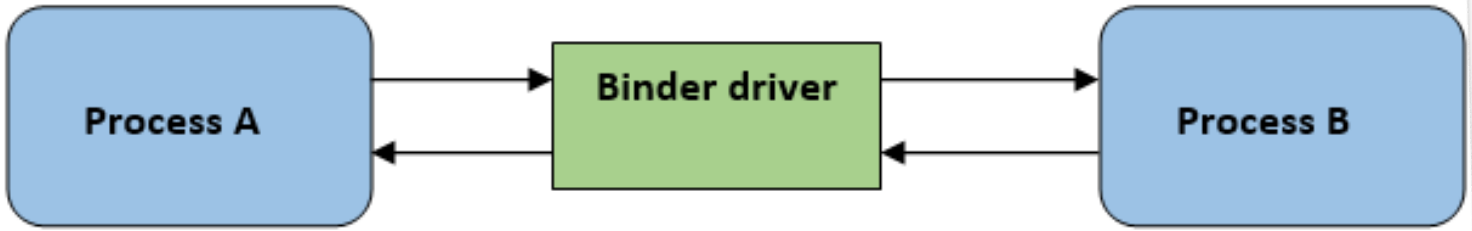
Application Signing

(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 #
```

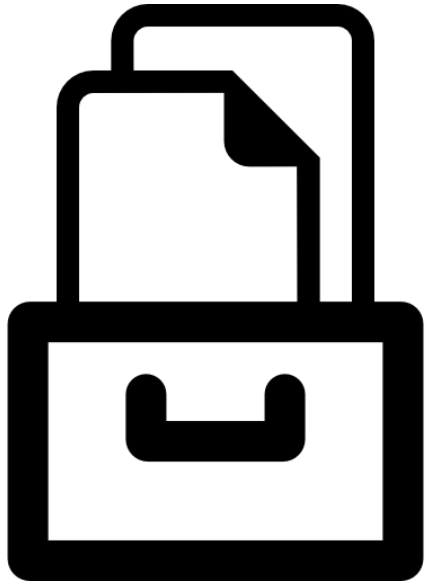
/data/data/com.android.browser

/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

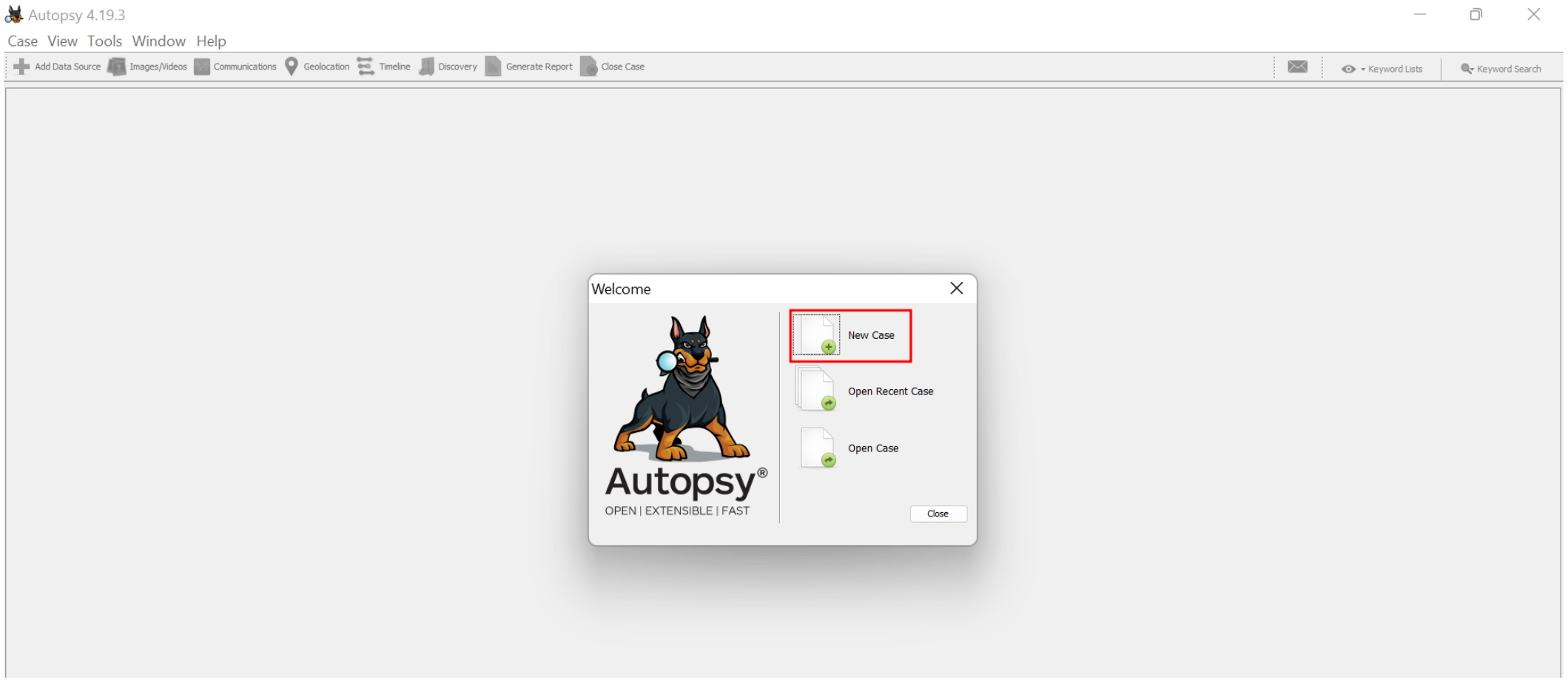
İmaj Alma (Acquisition)

- **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 .

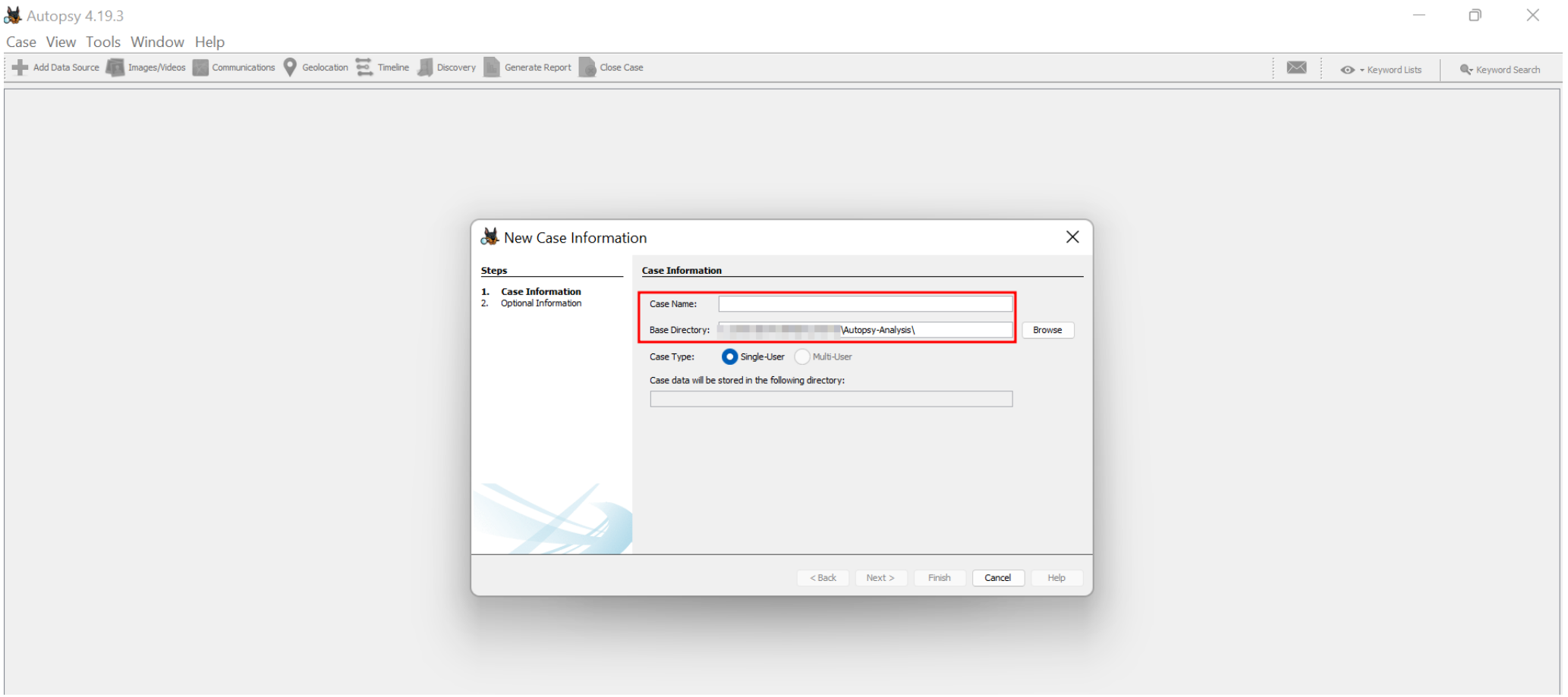


Android Forensic Toolları

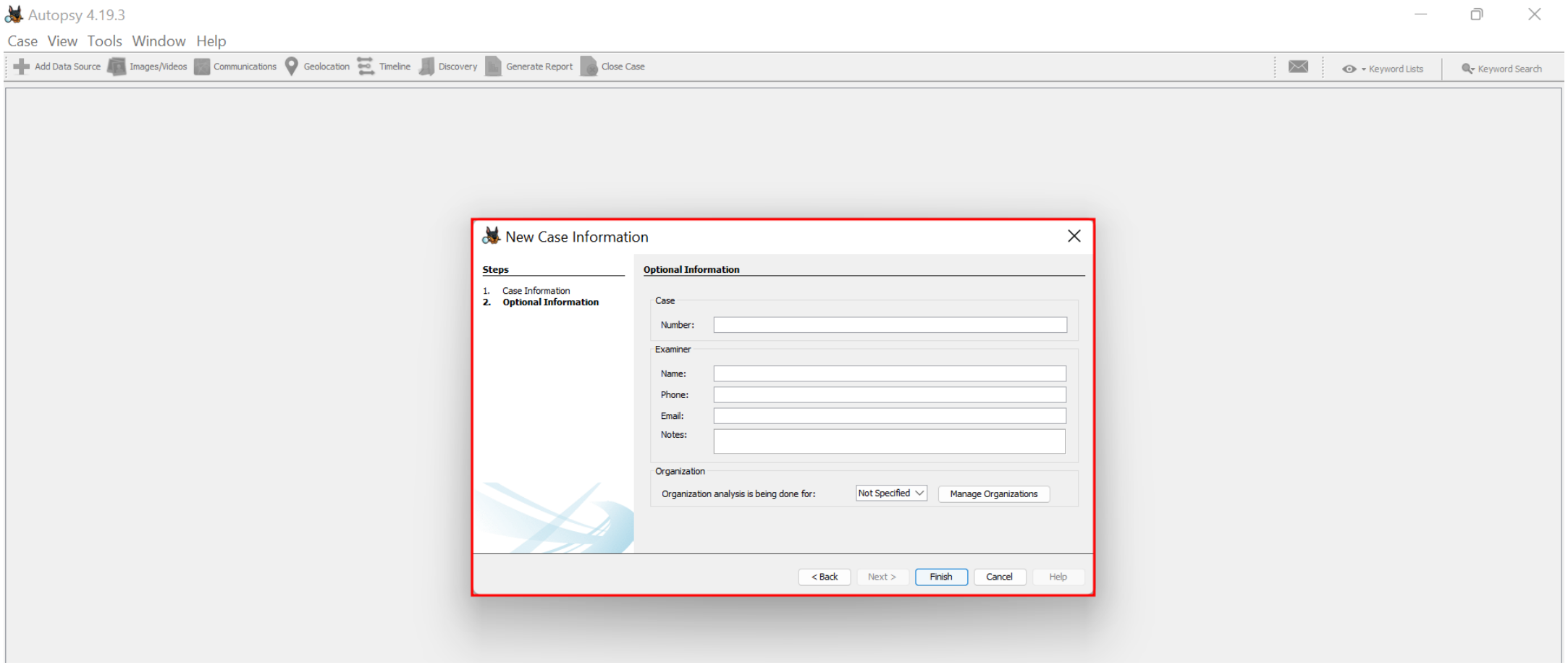
Autopsy Dosya Analizi



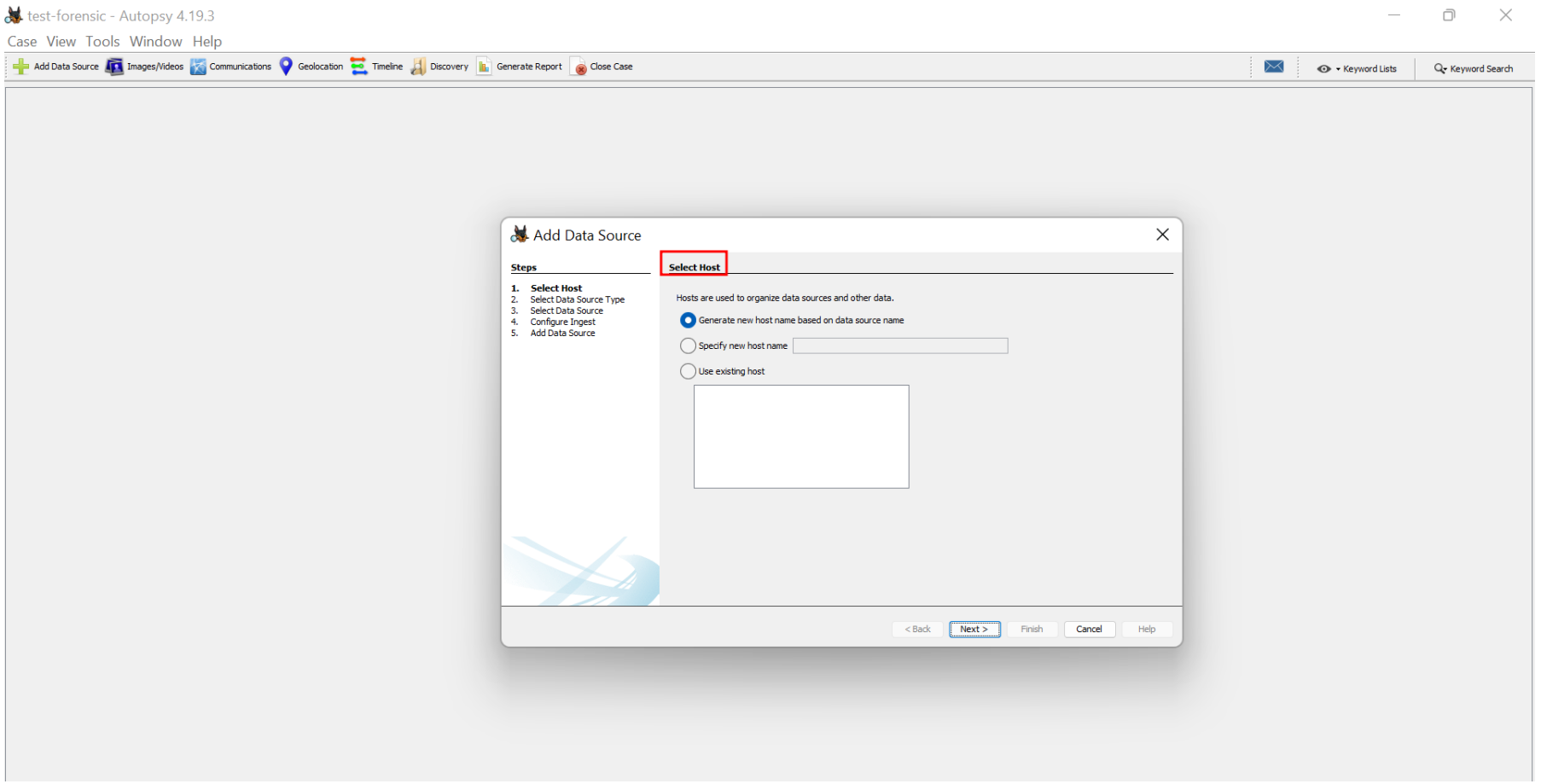
Autopsy Dosya Analizi



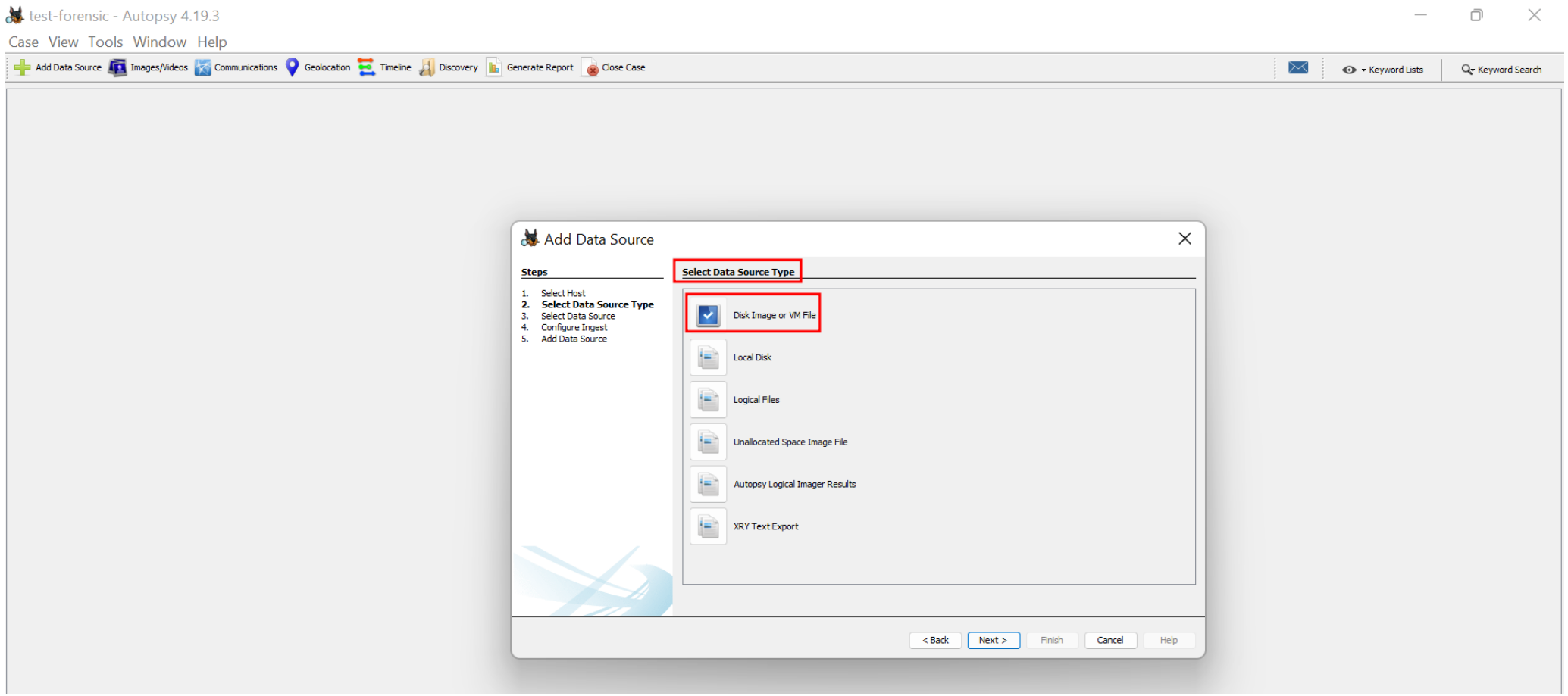
Autopsy Dosya Analizi



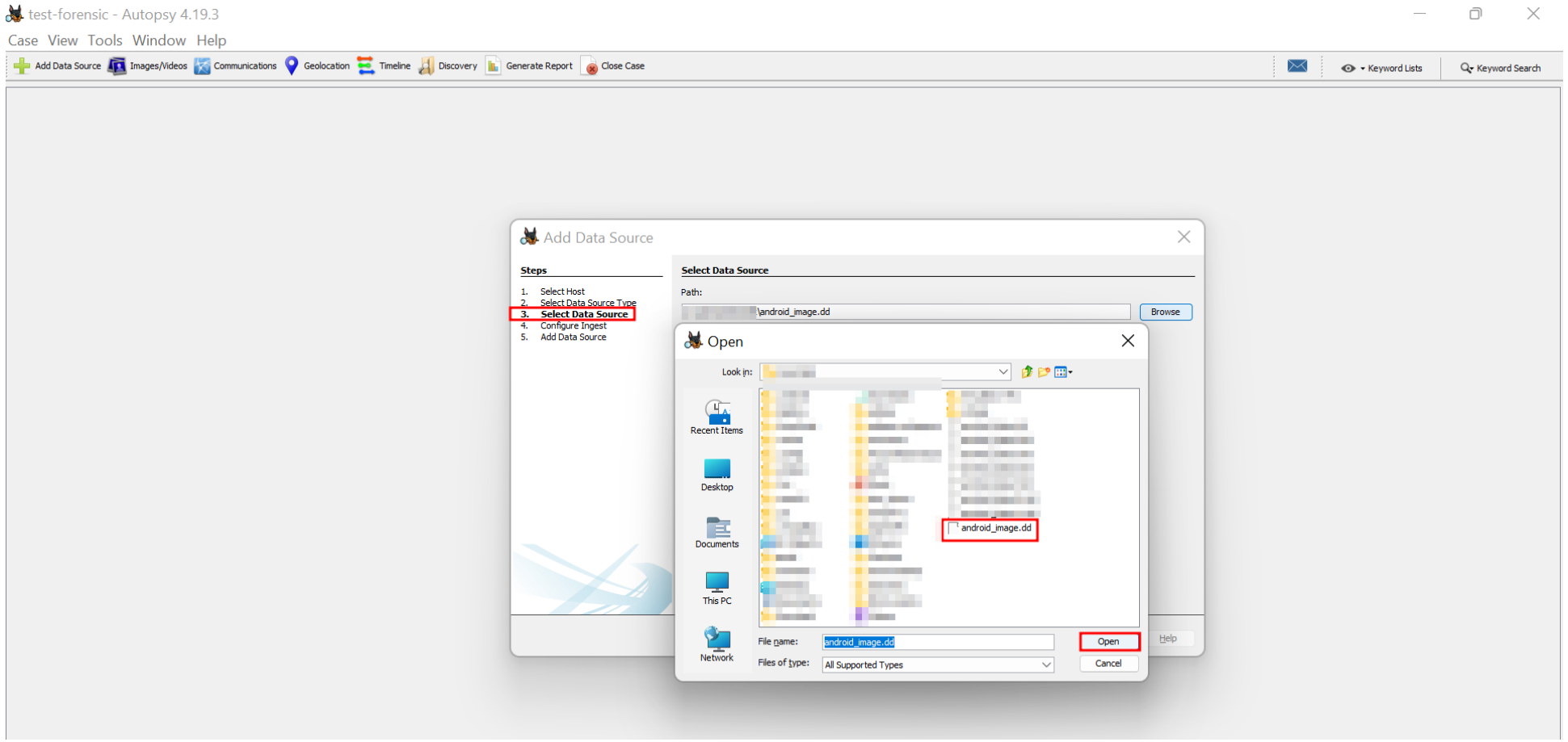
Autopsy Dosya Analizi



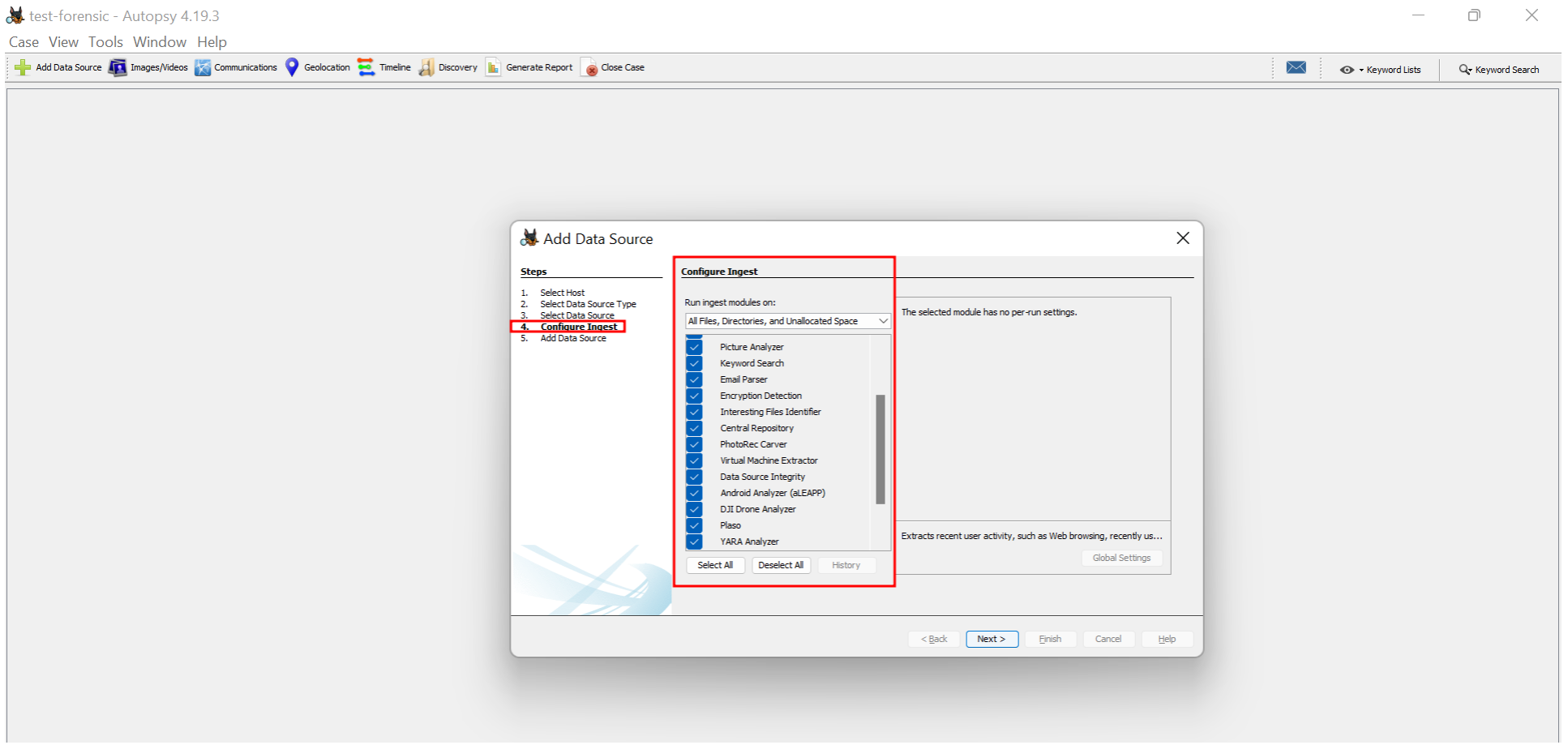
Autopsy Dosya Analizi



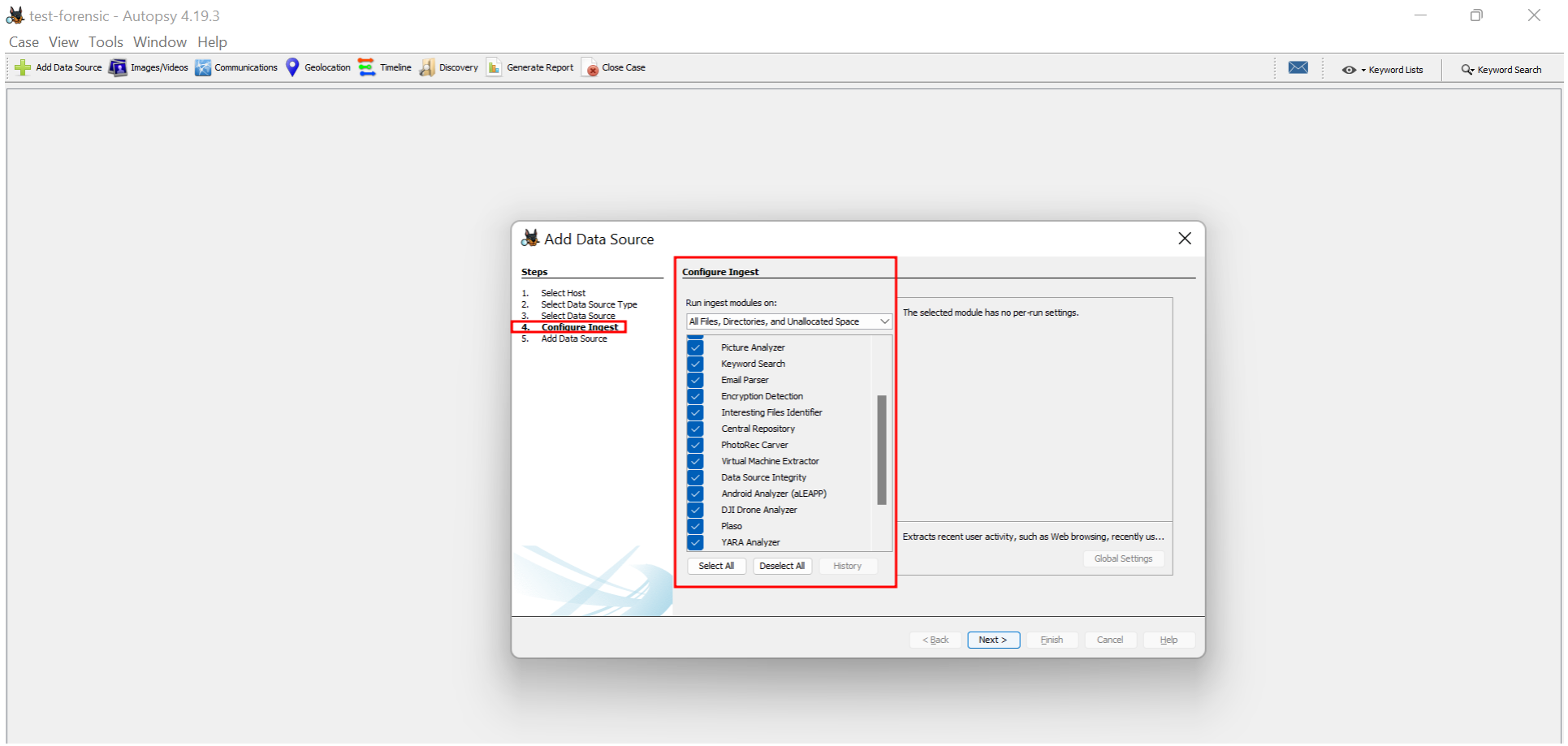
Autopsy Dosya Analizi



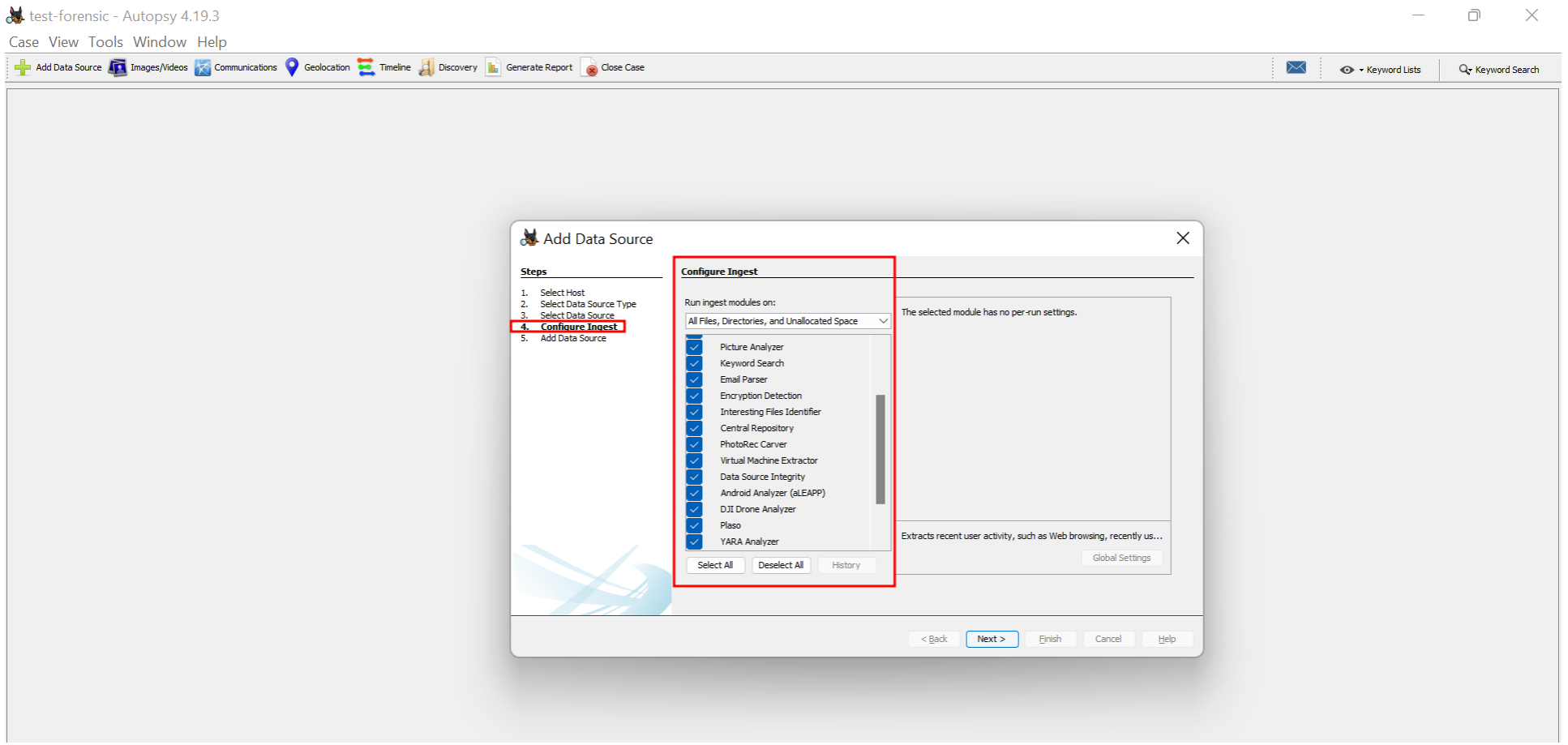
Autopsy Dosya Analizi



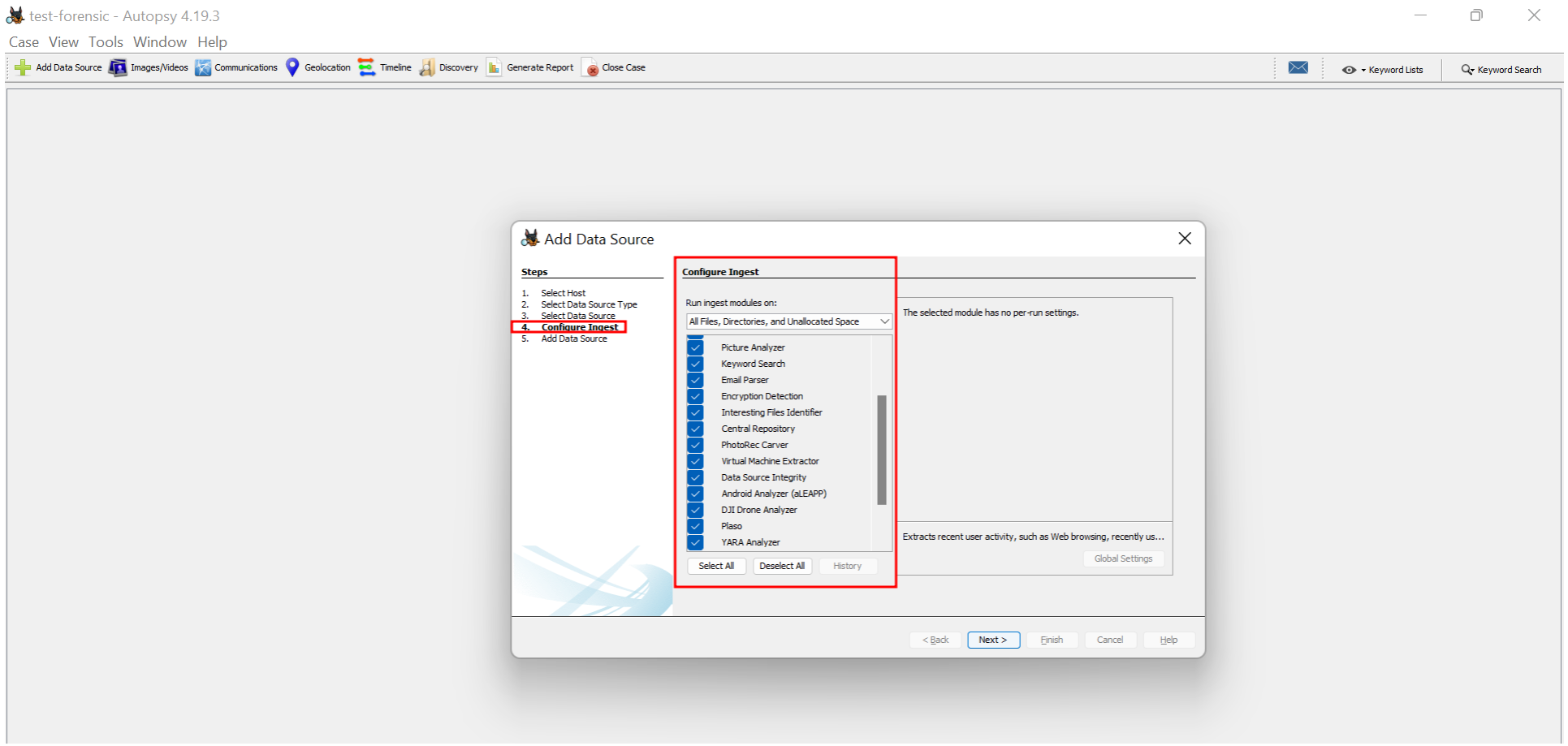
Autopsy Dosya Analizi



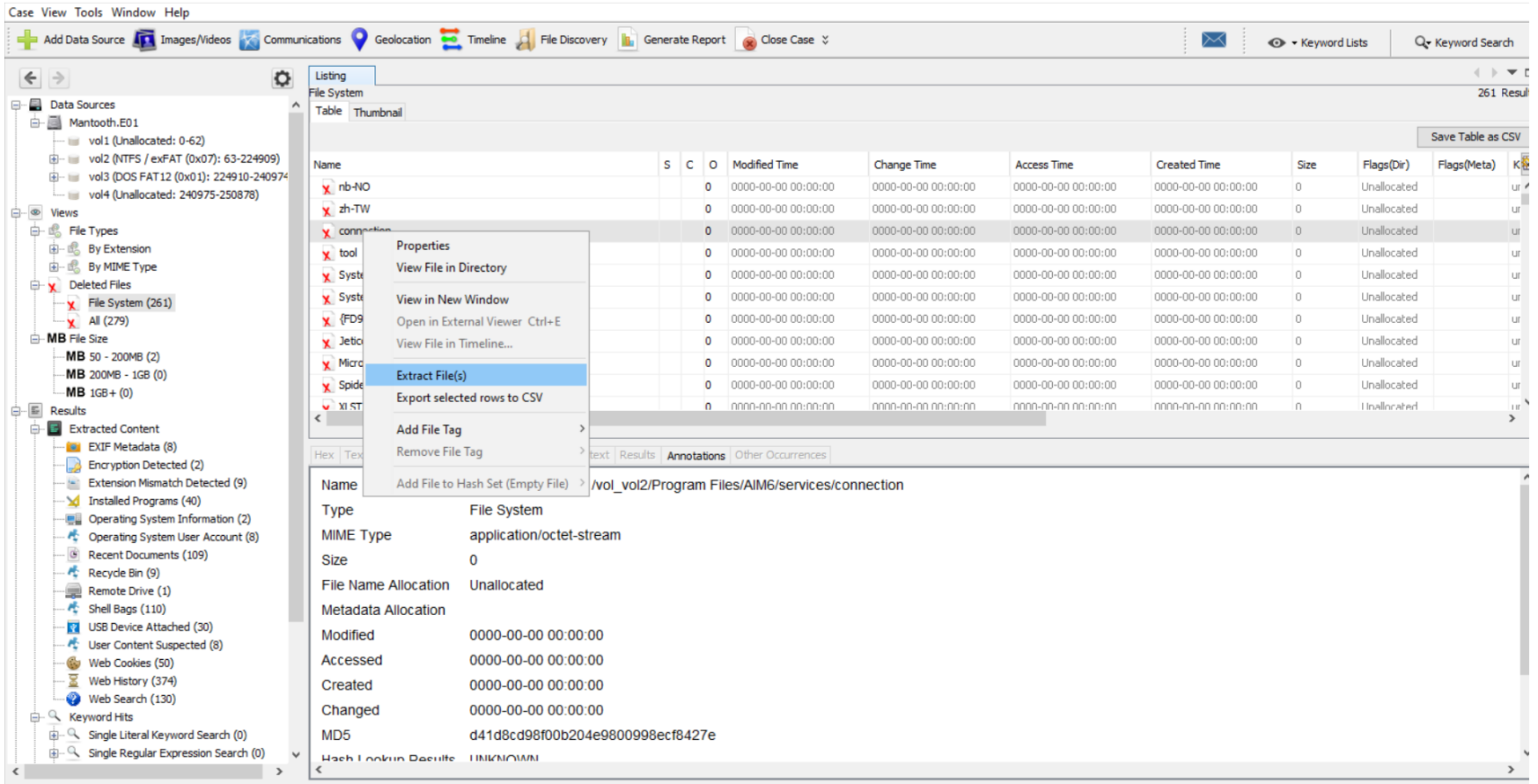
Autopsy Dosya Analizi



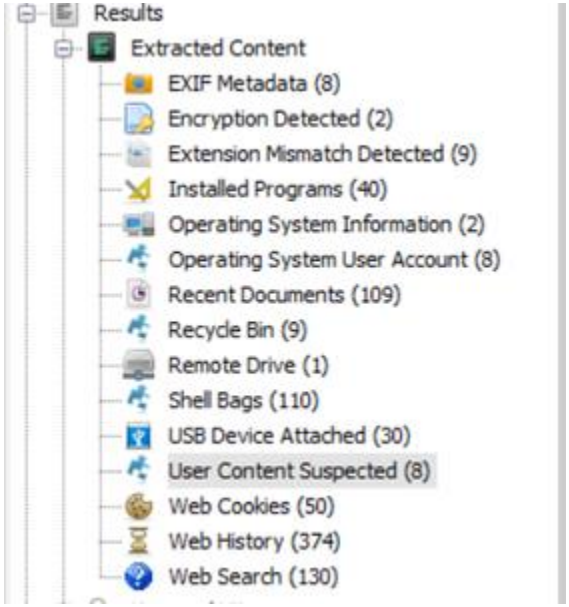
Autopsy Dosya Analizi



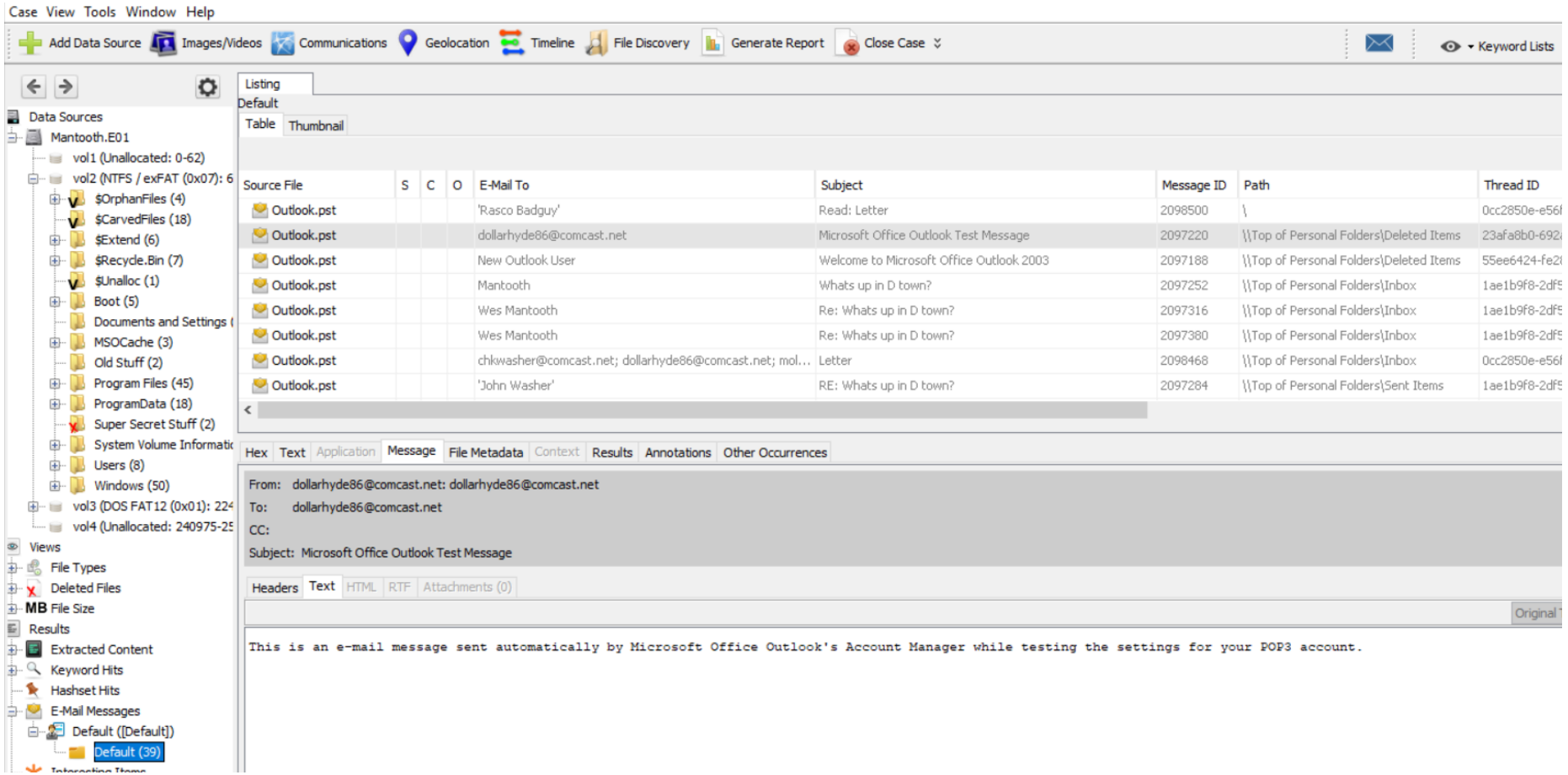
Autopsy Dosya Analizi



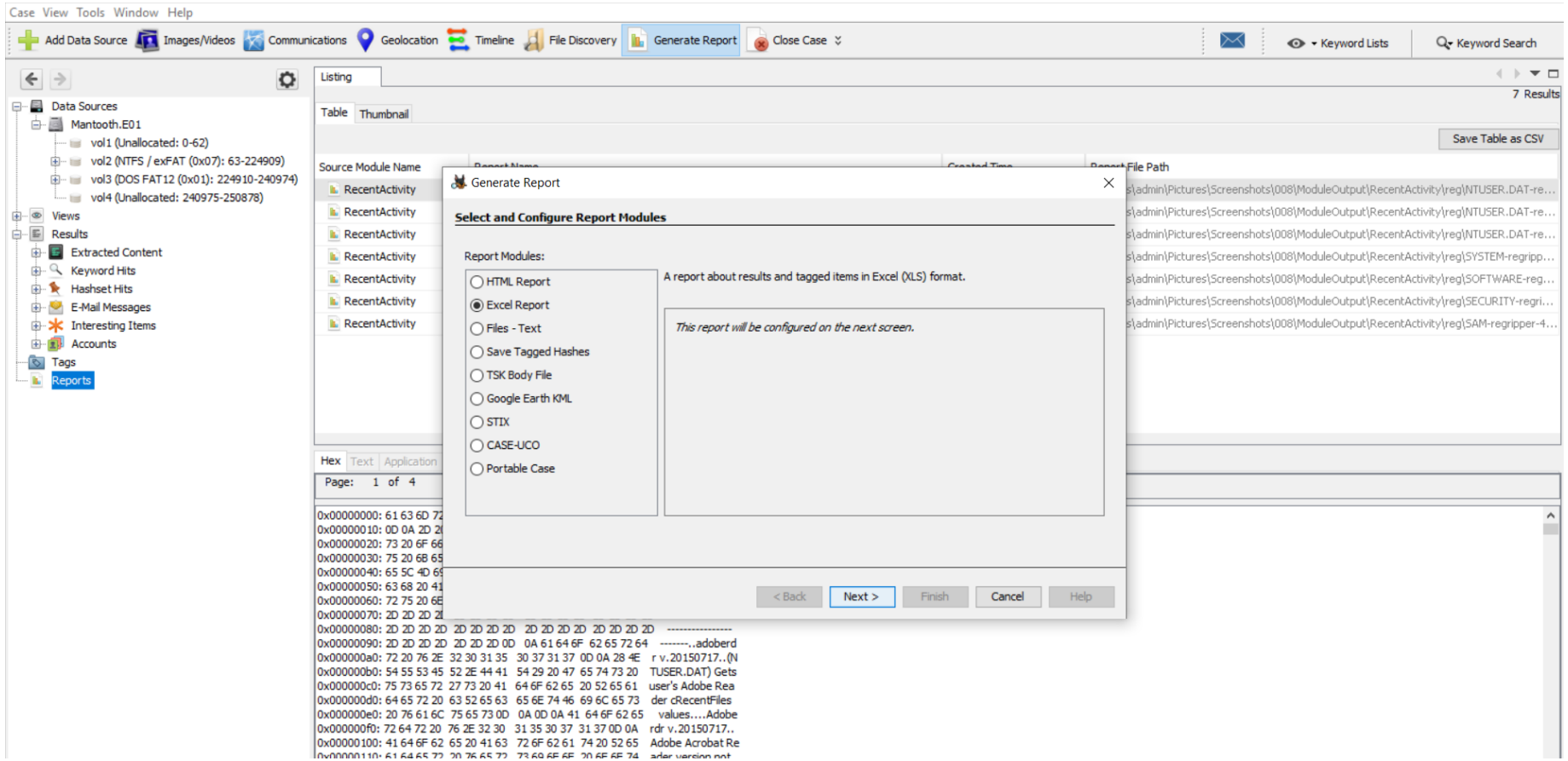
Autopsy Dosya Analizi



Autopsy Dosya Analizi



Autopsy Dosya Analizi



Thank you!
Any Questions?

PurpleBox

www.prplbx.com