Recovering Files From Forensic Images

Цел: Да се вратат назад во употреба фајлови кои се дел од форензичката слика.

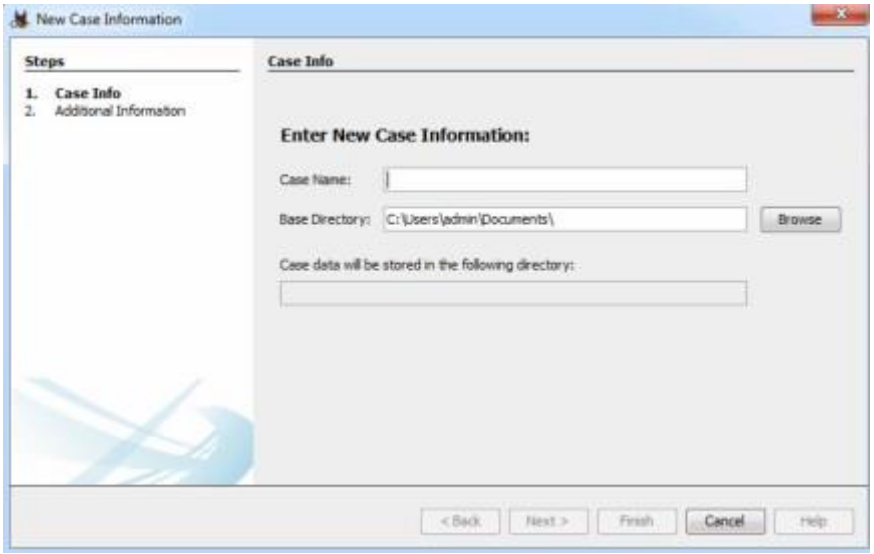
Примена: Фајловите од форензичката слика може да се искористат како докази против напаѓачот.

Дел 1:

Потребни алатки: Autopsy

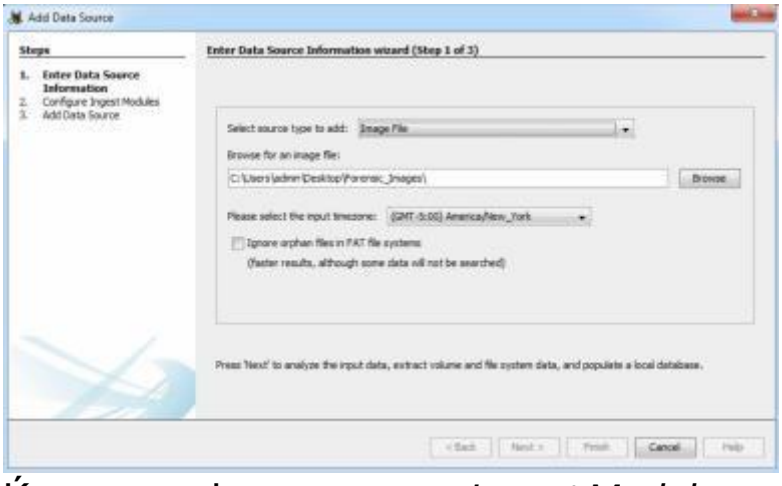
Чекори:

1. Инсталирајте ја алатката
2. Симнете го фајлот drive2.E01 од дадениот линк и поставете го на Desktop.
3. Отворете ја Autopsy алатката.
4. Во “*Welcome*” прозорецот кликнете на копчето “*Create New Case”*.
5. Во делот за “*New Case Information*” додади го името на случајот (case name) и постави го директориумот каде ќе се зачува case data.

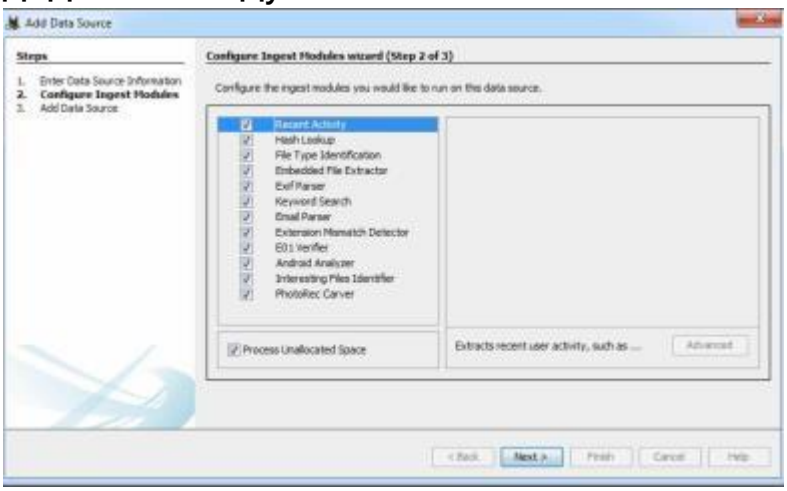


6. Кликни на “*Finish*” копчето.

7. Во прозорецот “*Add Data Source*” кој ќе ви се појави, додадете ја локацијата на drive2.E01 форензичката слика и кликнете на “*Next*” копчето.

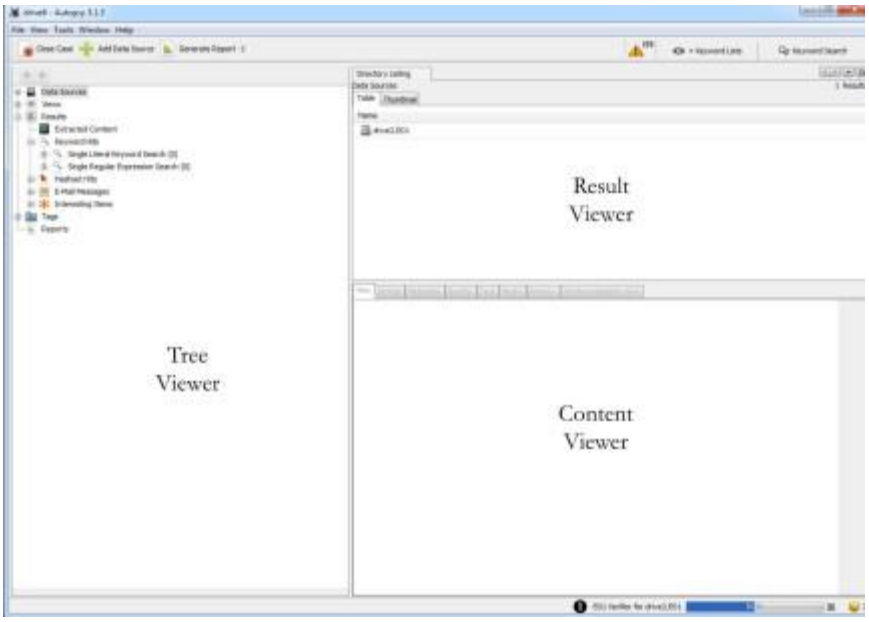


8. Ќе ви се појави листа од *Ingest Modules* кои автоматски ќе се извршат со вчитувањето на датотеката. Селектирајте ги дадените модули како што е на сликата.

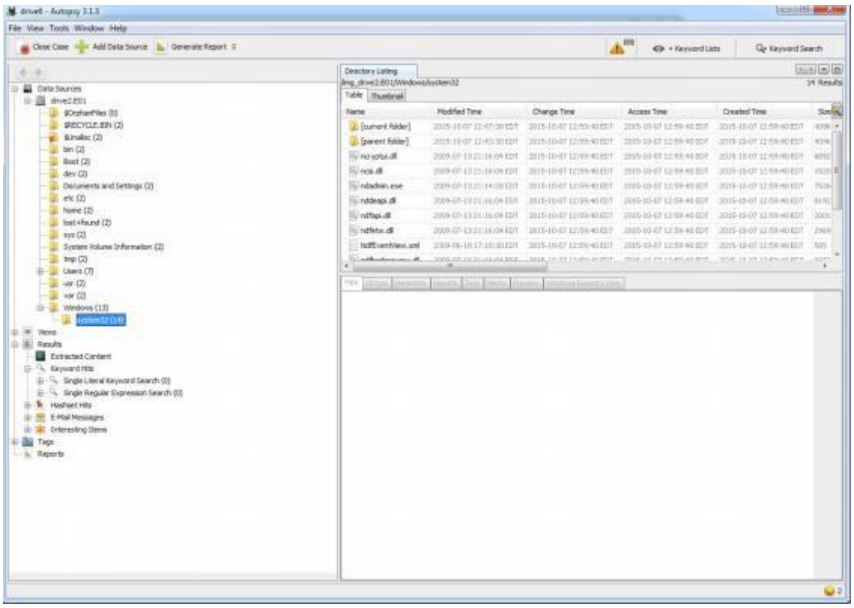


9. Кликнете на “*Finish*”.

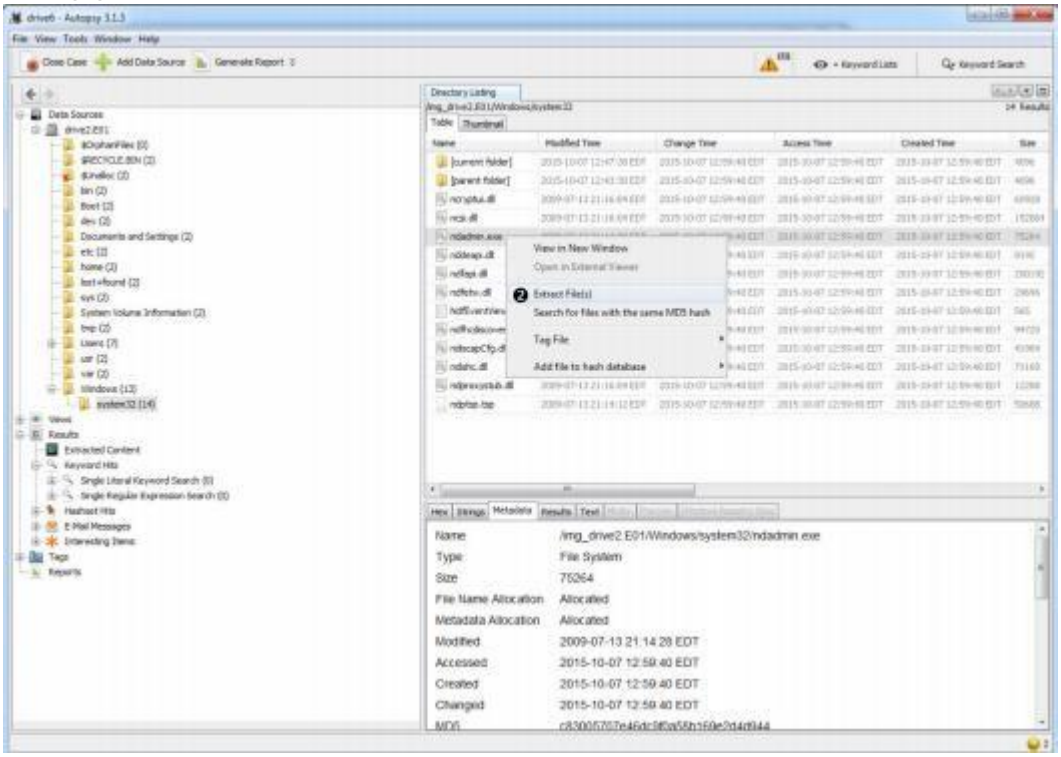
10. Кога ќе ви се вклучи прозорецот на Autopsy ќе ви се појават три панели Tree Viewer, Result Viewer и Content Viewer.



11. Во делот на Tree Viewer кликнете на (+) симболот кај *Data Sources* и кликнете на drive02.E01.
12. Навигирајте се до *C:\Windows\system32* како на сликата.



13. Десен клик на nsadmin.exe и селектирајте “*Extract File(s)”* како на сликата.



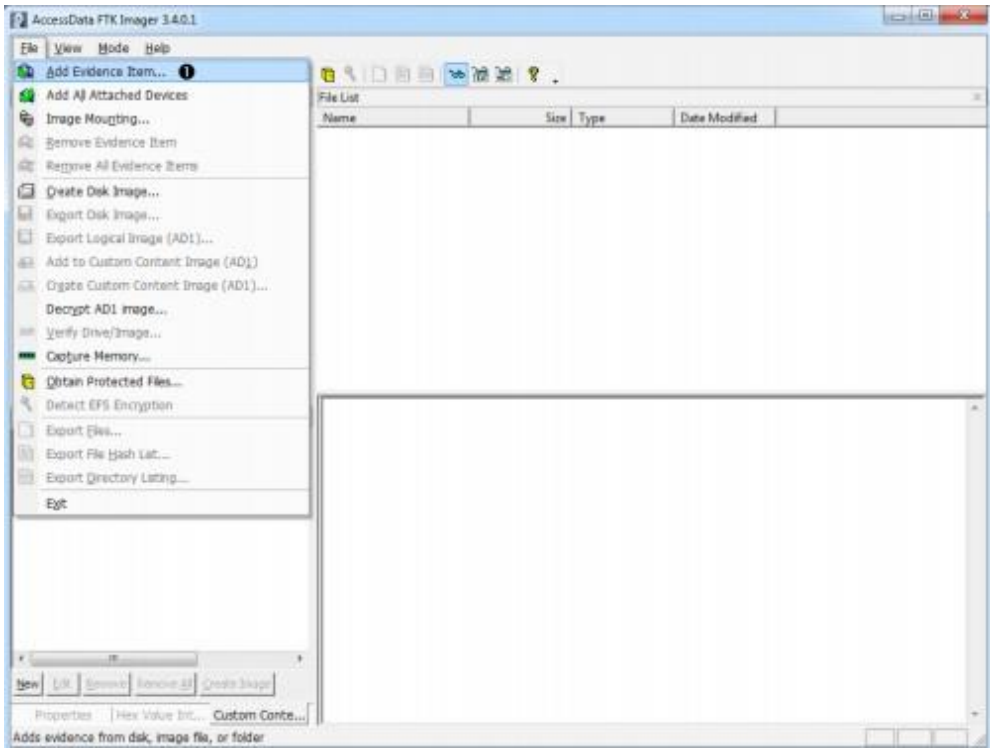
14. Наведи ја локацијата каде ќе го зачувате фајлот.

Дел 2:

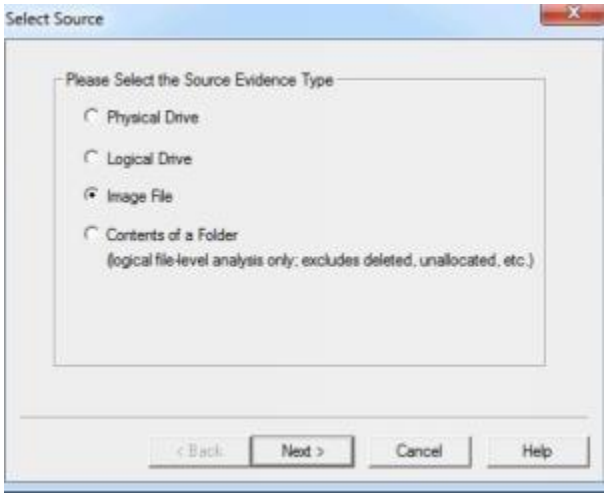
Потребни алатки: FTKImager

Чекори:

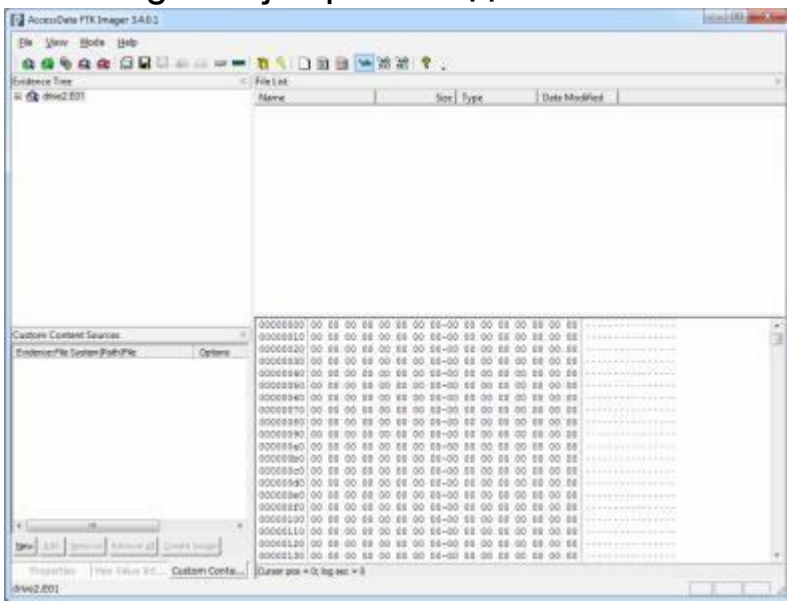
1. Инсталирајте ја алатката.
2. Симнете го фајлот drive2.E01 од дадениот линк и поставете го на Desktop.
3. Отворете ја FTKImager алатката.
4. Од главното мени селектирајте “*File*”, потоа “*Add Evidence Item*” како на сликата.



5. Во прозорецот кој ќе ви се појави изберете “*Image File*” а потоа кликнете на “*Next*” копчето.



6. Навигирајте се до десктопот и селектирајте ја drive2.E01 форензичката слика и кликнете на “*Finish*” копчето.
7. FTKImager ќе ја прикаже датотеката како на сликата.



8. Кликнете на (+) симболот кај drive2.E01.
9. Навигирајте се до *\root\Windows\system32*.
10. Десен клик на nsadmin.exe и селектирајте *“Extract File(s)”* како на сликата.
11. Наведи ја локацијата каде ќе го зачувате фајлот.

12. Откако фајлот ќе биде експортиран ќе ви се појави следниот прозорец.