Форензика оперативних система

Доказни материјал укључује следећа меморијска складишта:

- Чврсти диск произвођача Seagate, модела ST1000DM010 и серијског броја 3660619402182, извађеног из кућишта директора Богољуба Гагића.
- Чврсти диск произвођача SYNOLOGY, модела HAT5300-12T и серијског броја 4711174724130, извађеног из кућишта запосленог Павла Пандуровића.

Форензичке слике поменутих меморијских складишта налазе се на локацији Documents/ ForenzickeSlike у оквиру форензичке радне станице LDF Kali Linux (виртуелне машине).

У циљу разрешења случаја спровести следећи поступак:

1. Извести све кошнице Windows регистра из чврстог диска Богољуба Гагића. (0.5 бодова)
2. Применом алата RegRipper над кошницом System пронаћи доказ да је USB флеш меморија, која припада Павлу Пандуровићу, била маунтована на рачунару Богољуба Гагића (0.5 бод).
3. Применом алата RegRipper над кошницом Software пронаћи доказ да се програм за логовање корисничког уноса (енг. *keylogger*) покреће на рачунару Богољуба Гагића након покретања оперативног система (1 бод).
4. Анализом конфигурационе датотеке оперативног система Linux, која се налази на чврстом диску Павла Пандуровића пронаћи апликацију за директну комуникацију која се покреће аутоматски након покретања оперативног система (1 бод).