Форензика масовне меморије

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 Western Digital, модела WD10SPZX и серијског броја 718037845319, извађеног из кућишта запослене Душанке Свиларевић.
- Чврсти диск произвођача SYNOLOGY, модела HAT5300-12T и серијског броја 4711174724130, извађеног из кућишта запосленог Павла Пандуровића.
- USB флеш меморија произвођача SanDisk, модела Cruser Force и серијског броја 0xd585e28 преузета од запосленог Павла Пандуровића.

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

У циљу разрешења случаја спровести следећи поступак:

1. Сав доказни материјал завести у документу „Ланац доказа” и идентификовати партиције и системе датотека којима су партиције форматиране на свим меморијским складиштима. (0,5 бодова)
2. Анализом чврстог диска рачунара извађеног из кућишта директора Богољуба Гагића, пронаћи малициозни софтвер помоћу кога је злонамеран запослени могао да дође до креденцијала за приступи веб сервису за вођење евиденције о поласцима камиона. (1 бод)
3. Аналзизом чврстог диска извађеног из кућишта запосленог Павла Пандуровића пронаћи и и извести сумњиве датотеке у application/pdf формату чија екстензија не одговара датом формату. (0,5 бодова)
4. Анализом USB флеш меморије преузете од запосленог Павла Пандуровића утврдити њен садржај. (0,5 бодова)
5. Анализом чврстог диска извађеног из кућишта запосленог Павла Пандуровића пронаћи обрисане датотеке сумњивог садржаја у jpg формату од 100 до 150 KiB. (0,5 бодова)