Форензика апликација

Доказни материјал укључује следећа меморијска складишта:

- 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.

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. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи који веб претраживач је коришћен, анализирати и документовати резултате претраге везане за туристичке агенције и дестинације. (0.5 бод)
2. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи мејл клијента који је коришћен, анализирати мејлове који су везани за контекст путовања, документовати учеснике у комуникацији (њихове мејл адресе), време слања порука, садржај порука и прилоге, уколико постоје. (1 бод)
3. Претходно пронађене датотеке које су биле прикачене као прилог унутар пронађених мејл порука извести, анализирати садржај и метаподатке докумената. Утврдити да ли је реч о авионским картама за одређену дестинацију и уколико јесте, документовати назив документа, компанију која је издала карту, на чије име гласи карта, за коју дестинацију је везана, датум и време лета и који је формат документа. (0.5 бода)
4. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи, анализирати и документовати мејлове везане за малициозни програм keylogger и извештаје које је послао програм. (0.5 бода)
5. Анализирати масовну меморију прикупљену са рачунара Душанке Свиларевић. Пронаћи који веб претраживач је коришћен, анализирати и документовати резултате претраге везане за куповину авионских карата. (0.5 бода)