Форензика радне меморије

Доказни материјал укључује следеће форензичке копије:

- Прикупљена рам меморија са рачунара запослене Душанке Свиларевић на ком је подигнут WindowsXP оперативни систем, помоћу FTKImager алата.
- Прикупљена рам меморија са рачунара запосленог Павла Пандуровића на ком је подигнут Ubuntu 14.04 оперативни систем, помоћу AVML алата.
- 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. Анализом радне меморије прикупљене са рачунара Павла Пандуровића пронаћи, анализирати и документовати активне процесе везане за апликације за директну комуникацију. (0,5 бодова)
2. Анализом радне меморије прикупљене са рачунара Павла Пандуровића пронаћи, анализирати и документовати сумњиве команде које је корисник уносио у терминал, а које указују на коришћење стеганографских алата и алата за криптовање фајлова, партиција, дискова. (1 бод)
3. Пронаћи све AES кључеве који се налазе у радној меморији прикупљеној са рачунара Павла Пандуровића. (0.5 бодова)
4. Анализом радне меморије прикупљене са рачунара Душане Свиларевић пронаћи, анализирати и документовати процесе који су покренути, а који нису системски. (0,5 бодова)
5. Доћи до датотека којима је руковао Павле Пандуровић током спровођења команди из задатка 2. (0,5 бодова)