ZADÁNÍ SEMINÁRNÍ PRÁCE

Vaším seminárním úkolem bude zpracovat report o forenzní analýze na základě následujícího zadání:

Legenda:

1. Popis případu:
Policie vyšetřuje podezření ze spáchání zvlášť závažného trestného činu terorizmu. Jedná se o podezření, že skupina osob pracuje na přípravě extrémně nebezpečného nástražného výbušného systému s velkým účinkem. Byl zadržen USB flash-disk, na kterém by mohly být uloženy nějaké informace o tomto výbušném systému.
2. Zadání:
Prověřte, zda se na předloženém USB Flash-disku nachází nějaké informace (textové, zvukové nebo obrazové informace) o výbušninách, případně jiné informace o zbraních hromadného ničení. V kladném případě uveďte další skutečnosti, které by se zjištěnými informacemi měli nějakou souvislost.
3. Předmět ke zkoumání:
1 ks USB Flash-disk zelené barvy plastový, s označením ADATA UV220/16GB.

Prostředky, které lze pro řešení použít:

Pro řešení zadání použijte vlastní počítač (z důvodu nutnosti existence administrátorského oprávnění k práci se speciálním forenzním SW).

Pro řešení je doporučeno použít SW:
- **FTK Imager** od firmy AccessData (volně ke stažení)
- **Autopsy** forenzní SW (opensource)
Oba uvedené programy lze využít v prostředí MS Windows i Linux.
Lze použít i další vhodné programové vybavení, použití kterého je však potřebné předem konzultovat případně zdůvodnit.
Postup řešení podrobně zadokumentujte ve výsledném reportu.
Při řešení postupujte v souladu s doporučeními pro digitální forenzní analýzu.
Rozsah výsledného reportu by neměl přesáhnout cca 10 stran.

Organizační pokyny:

Předmět zkoumání (předem připravený USB Flash-disk) je k dispozici u vyučujícího.

Pro realizaci seminární práce je nutné:
- instalovat na váš počítač program FTK Imager
- zapůjčit si u vyučujícího daný USB Flash-disk a pomocí programu FTK Imager pořídit forenzní obraz disku na váš počítač (pod dohledem vyučujícího). Tím získáte vstupní data pro vaši seminární práci.

Celá operace pořízení forenzního obrazu disku nepřekročí cca 10-15 min a lze ji

realizovat jak na přednáškách, tak na cvičeních v řádných termínech.

Seminární práci zpracujte do 15. 12. 2019 a výsledek uložte do odevzdávárny.

ASSIGNMENT OF SEMINAR WORK

Your seminar task will be to prepare a report on forensic analysis based on the following assignment:

Legend:

1. Description of the case:
Police are investigating suspicions of a particularly serious crime of terrorism. It is a suspicion that a group of people are working on the preparation of an extremely dangerous high explosive explosive system. A USB flash drive has been detained on which some information about this explosive system could be stored.
2. Assignment:
Check whether there is any information (text, audio or image) on explosives or other information on weapons of mass destruction on the USB flash drive. If so, please indicate any other facts that would be related to the information found.
3. Subject to be examined:
1 pc USB flash drive green plastic, marked ADATA UV220 / 16GB.

Means that can be used for the solution:

To solve the task use your own computer (because of the need to have administrator privileges to work with special forensic SW).

For the solution it is recommended to use SW:
- **FTK Imager** by AccessData (free download)
- **Autopsy** forensic SW (opensource)
Both programs can be used in MS Windows and Linux.
Other suitable software may be used, but the use of such software must be consulted in advance or justified.
Document the examination procedure in detail in the final report.
Follow the recommendations for digital forensic analysis.
The size of the resulting report should not exceed about 10 pages.

Organizational instructions:

The subject of examination (pre-prepared USB flash drive) is available from the teacher.

To carry out the seminar work it is necessary to:
- install FTK Imager on your computer
- borrow the USB Flash-Drive from the teacher and use the FTK Imager software to take a forensic image of the drive onto your computer (under the supervision of the teacher). This will give you input data for your seminar work.

The whole operation of acquiring a forensic image of a disc does not exceed about 10-15 minutes and can be realized both in lectures and in exercises in due dates.

Work up the seminar work by December 15, 2019 and save the result in the delivery room (odevzdávárna).