1. **Milyen címet adna a ma érintőleg említett szakdolgozati témájának?**

Adatvédelem és belső biztonsági megoldások fejlesztése a mobileszközökkel szemben🡨ennek alapján az Olvasó szinte még bármire gondolhat, vagyis nem elég specifikus a cím (honnan, hová, miért, hogyan?)

**2. Mi lenne az alcím?**

A képrögzítésre alkalmas eszközök felügyeletének fejlesztése🡨a leíró munkát sejtető címe egyike sem jó, a cél a fejlesztés, de a címnek olyan kulcsszavakat kell tartalmaznia, melyek alapján a lényeg azonnal értelmezhető

**3. Hogyan nézzen ki a cím angolul?**

Data protection and internal security solutions for mobile devices

**4. Mi legyen az alcím fordítása angolra?**

Supervision of devices capable of recording images

**5. Miként írná le kb. 1000 karakterben a dolgozat lényegét (vö. kivonat) = célok, célcsoportok, hasznosság, feladatok, motiváció**

*Célok:* Képrögzítésre alkalmas eszközökkel történő, adatok engedély nélküli eltulajdonításának a megakadályozása.

Adatok képrögzítésre alkalmas eszközökkel történő engedély nélküli eltulajdonításának a megakadályozás🡨ez eddig a legjobb, legkonkrétabb cím-variáns

*Célcsoportok:* Minden olyan terület, ahol különösen fontos az adatok védelme. 🡨A mindenre utalás felesleges. Olyan marketing akciót senki nem finanszíroz meg, melyben a válaszadási esély a megszólítottak köréhez képes alacsony. Kik a leginkább érintettek, akik hajlandók lehetnek fizetni is a fejlesztés eredményeiért?

*Hasznosság:* Általánosságban elmondható, hogy a cégek (pl….) elsősorban a külső támadások megelőzésére fektetik a nagyobb hangsúlyt, ha IT biztonságról van szó. Azonban a belső támadásokkal jóval nagyobb károk keletkezhetnek az adatok (pl. …) lopásával, módosításával, törlésével, kémprogramok telepítésével. Az egyik potenciális veszélyt a külső adathordozók rejtik (pl. pendrive), mivel nincs szükség szaktudásra a használatukhoz, de ezek felügyeletére, kezelésére léteznek már hatékony megoldások (pl. …). Viszont a fényképezőgépekkel (egyéb képrögzítésre alkalmas eszközökkel: pl....) szemben, mint adatok lopására is alkalmas igen hatékony eszközzel szemben nem igazán vagyunk felkészülve..

*Motiváció:* A legnagyobb veszélyt, a mai (okos)mobiltelefonok jelentik. Képesek, adatok tárolására, kép és hangrögzítésre, programok futtatására, tehát tulajdonképpen egy jelentős funkcionalitással rendelkező számítógépről beszélhetünk. A legegyszerűbb és leggyorsabb adatszerzési módszerek egyike a fényképezés, (a hangrögzítés, …).

Természetesen a digitális és analóg minifényképezőgép is egy létező veszélyforrás lehet, így általánosságban a képek rögzítésére alkalmas eszközökkel szembeni védelemre helyezném a hangsúlyt.

*Feladatok:* Olyan szoftver fejlesztése, mellyel figyelhető, naplózható, a felhasználói tevékenység, mely riasztásra is képes, ha képet szeretnének készíteni egy megjelenítőről illetve a monitorról. Erre a legalkalmasabb hardver eszköz a (web)kamera, amellyel megfigyelhető a képrögzítési szándék is. (A kamera egyéb biztonsági feladatokat is ellátna, pl. azonosítás, beléptetés, automatikus képernyő zárolás, stb.) A kamera, illetve az azt vezérlő szoftver, felismerné a vele szemben álló optikát, majd megtörténne a riasztás, naplózás, és a felhasználó zárolása, letiltása… Új cím: Kémkedésre alkalmas optikai eszközöket, fényképezési szándékot felismerni képes webkamera-szoftver fejlesztés

Vagyis az optikai eszközök esetén egy-egy állókép-értelmezési/elemzési kihívás kezelése a feladat, míg a szándékot mozgókép (egymást követő sok mozgókép) alapján tervezi felismerni?

Az állóképek kapcsán ez a fejlesztés egy fajta captha-jellegű tanulási folyamat (neurális háló-fejlesztés) lenne? Vagy képesnek érzi magát arra, hogy pozitív és negatív esetek ismerete nélkül meg tudja alkotni a megfigyelő eszköz (lencse, objektív) felismerését (vö. gyanúgenerálás)? Hogyan lehet az okosszemüveget, a gomblyukba elhelyezett rejtett kamerát, stb. felismerni a nyilvánvaló fényképezési mozdulat és ennek eszköze felismerésétől? Vagy ez nem lesz cél?

6. Hogyan néz ki angolul (abstract) a magyar kivonat?