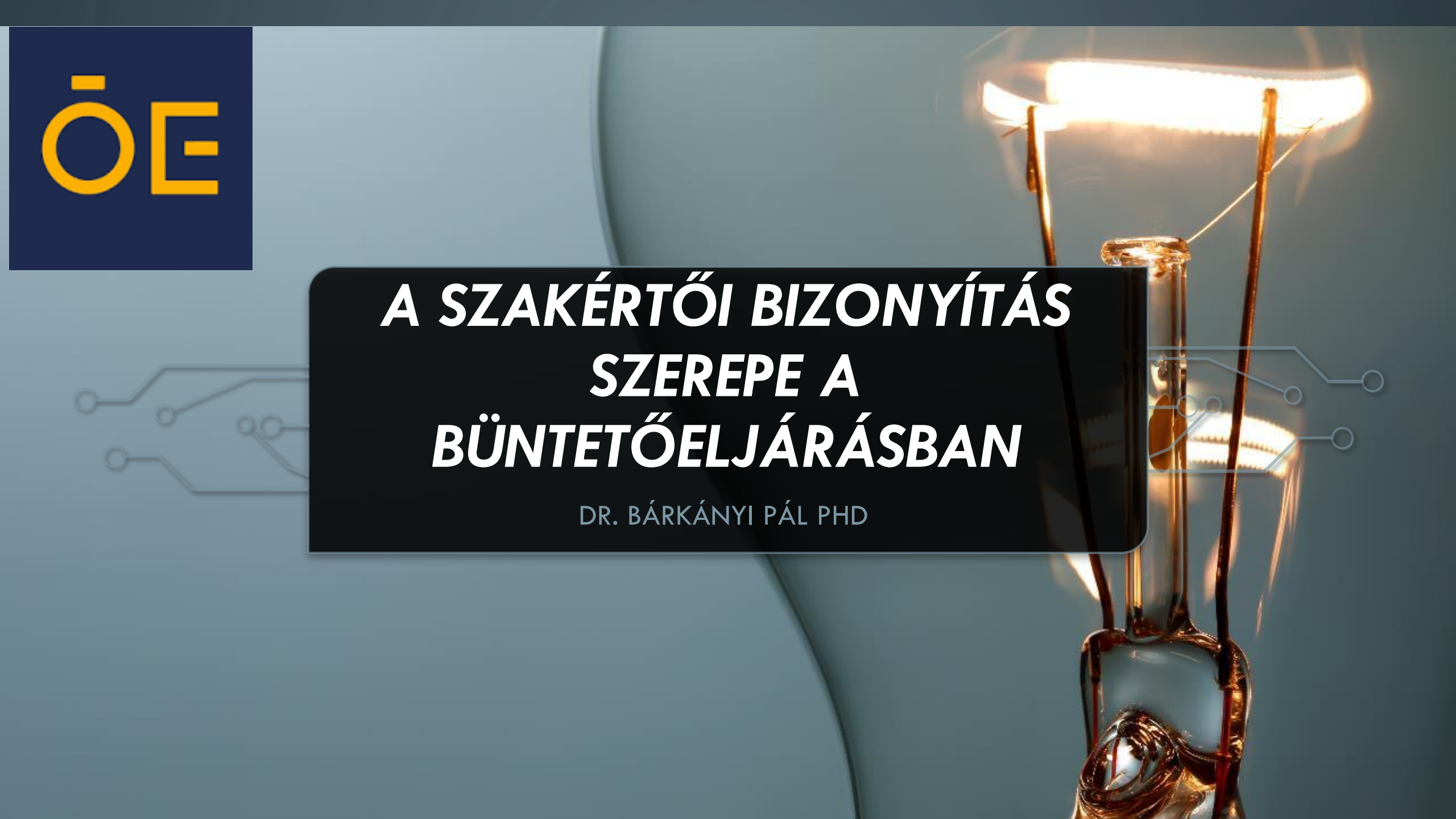
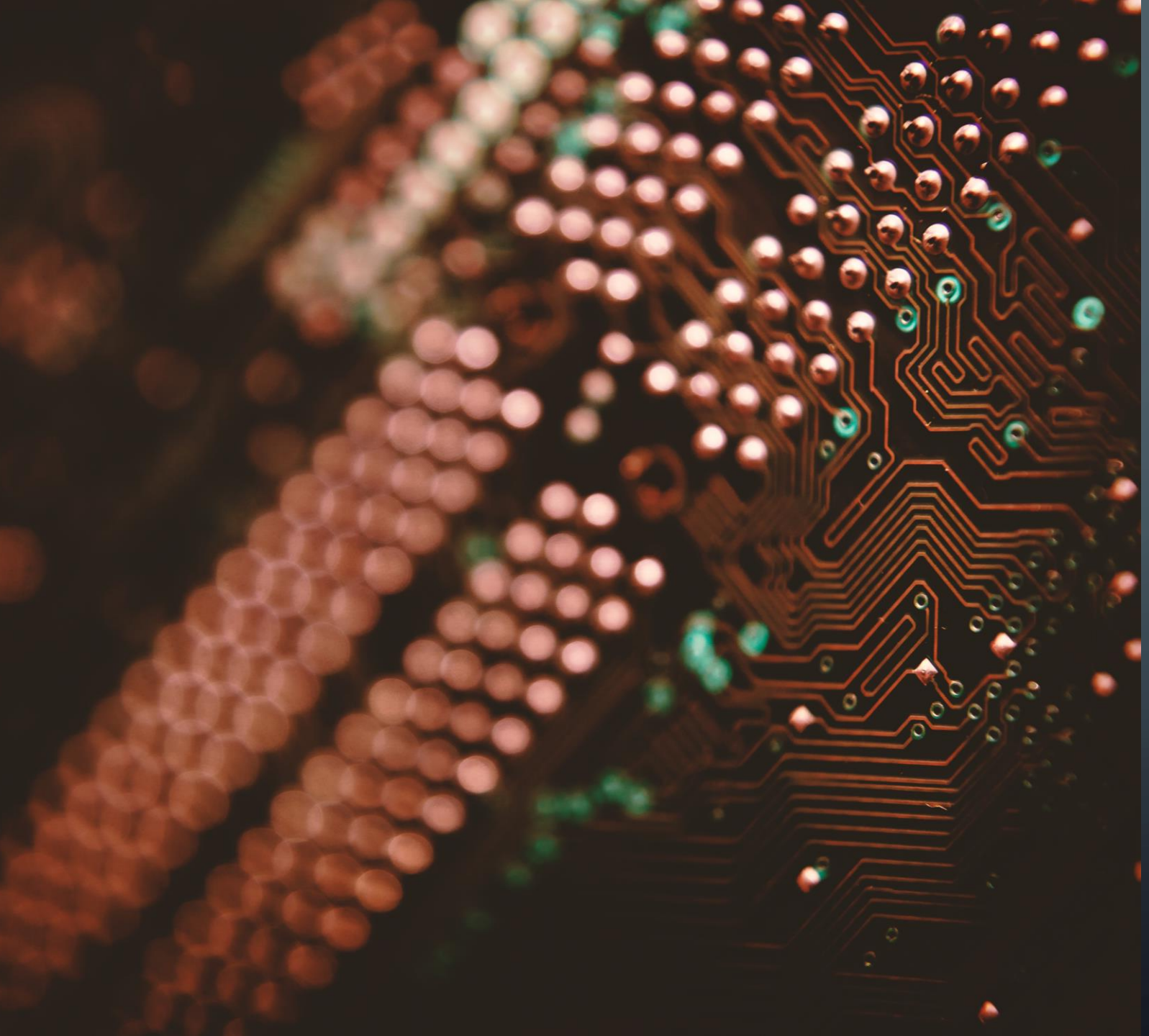
A SZAKÉRTŐI BIZONYÍTÁS SZEREPE A BÜNTETŐELJÁRÁSBAN

DR. BÁRKÁNYI PÁL PHD





AZ ELŐADÁS CÉLJA

- Ismertetni az informatikai igazságügyi szakértést, felvillantva néhány problémát
- Milyen feladatokat/tevékenységeket végez(het) egy informatikai igazságügyi szakértő
- Digitális forensics
- főbb technikákat...

LOCARD-FÉLE ANYAGÁTADÁSI SZABÁLY

Minden érintkezés nyomot hagy:

- tetthely
- elkövető
- áldozat

Nyom:

- lenyomat
- anyagmaradvány
- adatmaradvány

DAUBERT KRITÉRIUMOK

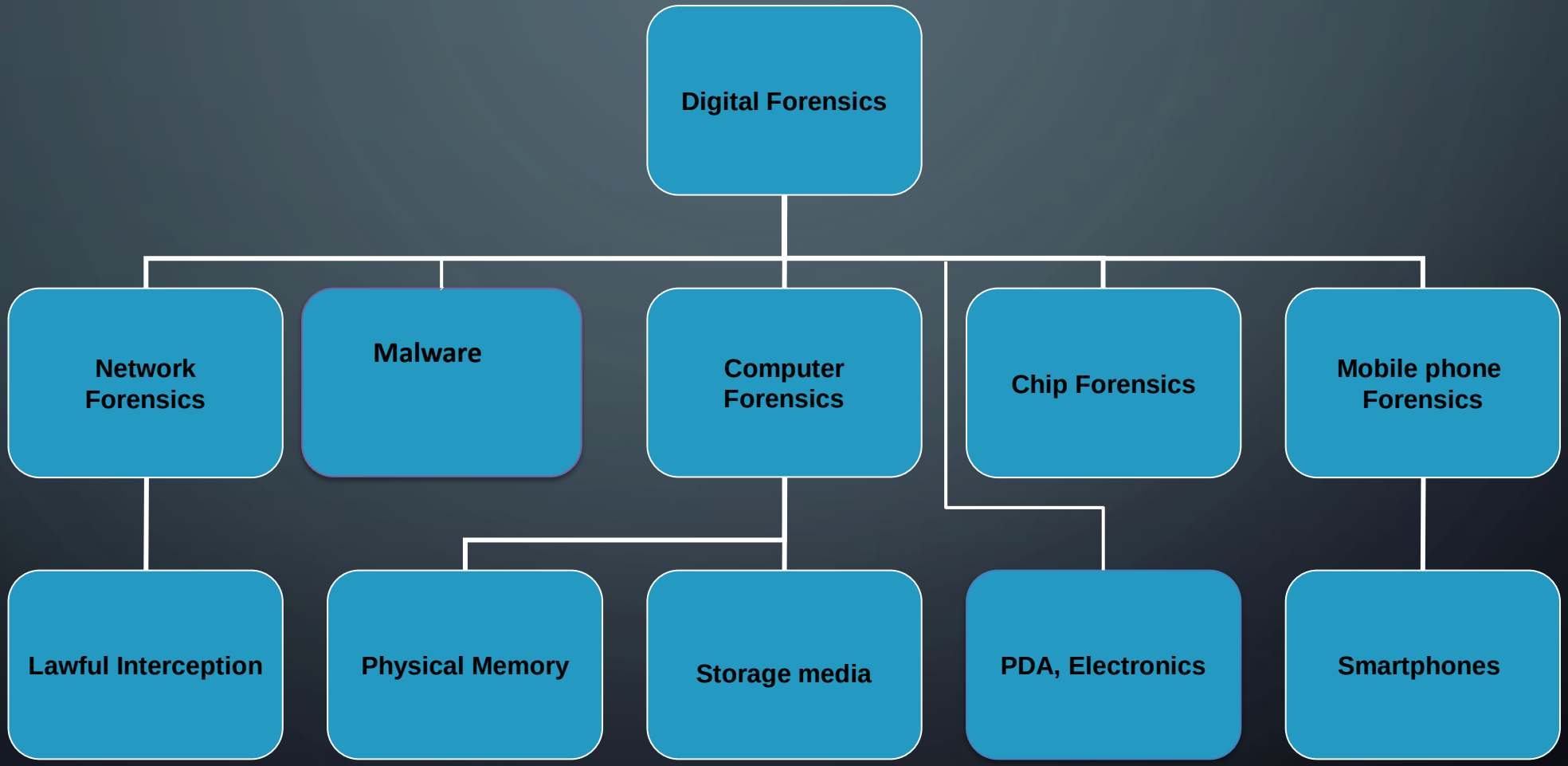
A bizonyítás **jogszerű,** ha

megfelel a jog szabályainak

A bizonyítás **szakszerű,** ha

- gyakorlatban is ellenőrzött (tesztelt) elméletre épül
- a tudományban elismert módon publikált
- ismert a hibaaránya
- a szakemberek tekintélyes közössége által elismert

DIGITAL FORENSICS



DIGITÁLIS BIZONYÍTÉKOK - ALAPELVEK

RELEVÁNS

az összegyűjtött bizonyítékoknak/anyagoknak relevánsnak kell lenniük a vizsgálat szempontjából,

MEGBÍZHATÓSÁG

ellenőrizhető és megismételhető folyamatok,

azonos intézkedések, módszerek, eljárások, feltételek,

MEGFELELŐSÉG

elegendő anyagot gyűjtöttek a vizsgálat elvégzéséhez.

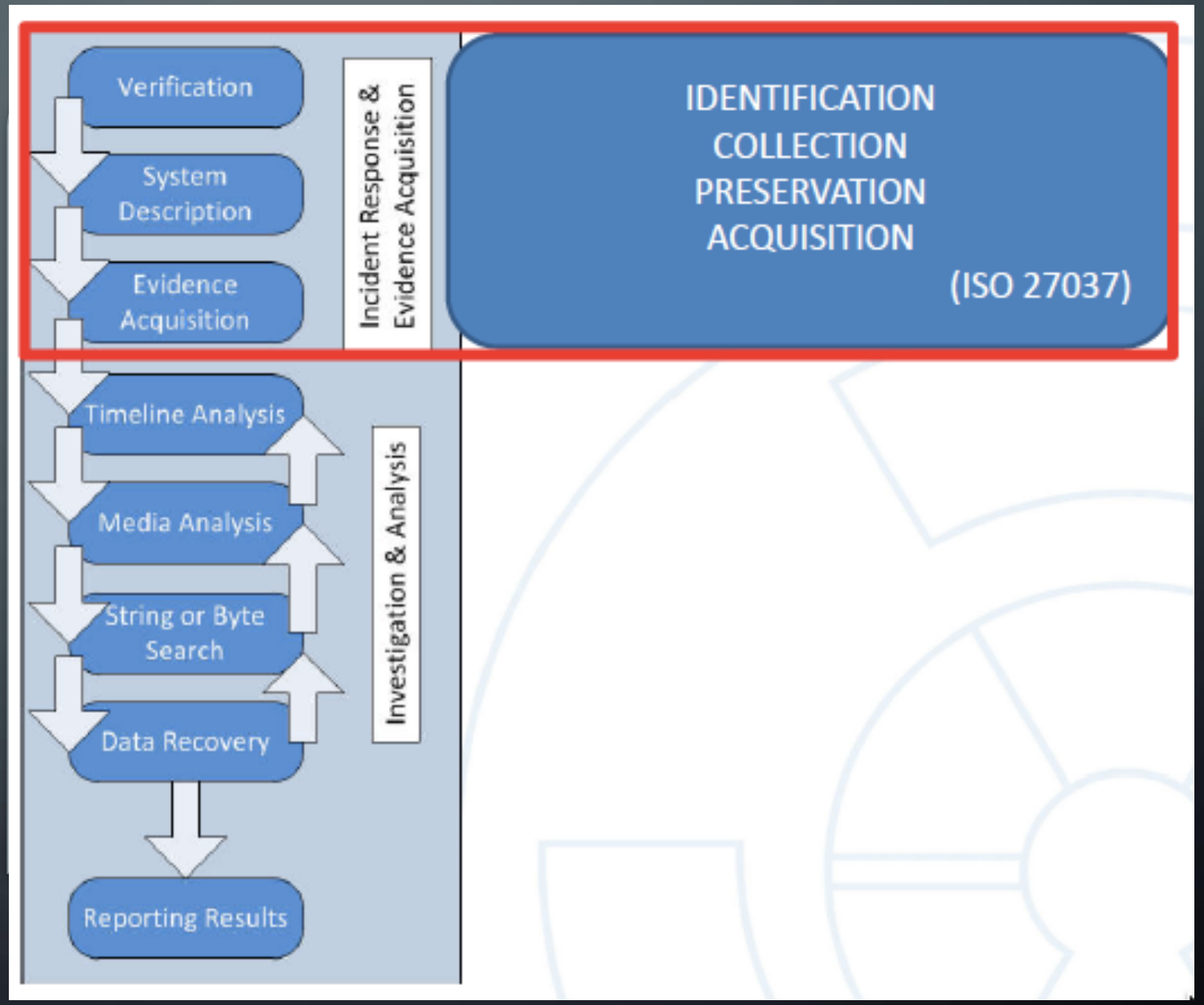
DIGITÁLIS BIZONYÍTÉKOK - ALAPELVEK

Digitális bizonyíték - bináris formában tárolt és továbbított információ, amelyre a bíróságon hivatkozni lehet;

Információt tárol:

- PC;
- Mobile;
- Tablet;
- Storage media;
- Electronic devices;
- Cameras;
- Dron;
- Etc.

A BIZONYÍTÉKGYŰJTÉS FÁZISAI



AZONOSÍTÁS

Logikai vs. fizikai forma

Prioritások meghatározása:

a bizonyítékok volatilitása szerint,

a bizonyítási érték relevanciája szerint,

az ok megértése - a sorrend meghatározása, a bizonyítékok befolyásolásának kockázatának minimalizálása és a bizonyítási érték maximalizálása érdekében.

Szisztematikus és alapos keresés

a rejtett bizonyítékokat.

ELLENŐRZÉS

Az első feladatok:

az eset valóban megtörtént?

az incidens még mindig folyamatban van?

ellenőrizni a jogosultságokat,

ellenőrizni a helyi folyamatokat,

ellenőrizni a rendszert,

BEGYŰJTÉS

Kérdések:

Gyűjtsük be vagy NE?

a választ az azonosítási folyamat adja meg,

DIGITÁLIS és NEM DIGITÁLIS bizonyítékok?

ON vagy OFF?

A következőkkel összhangban kell történni:

Az engedélyek szerint,

Törvények és joghatóság,

Különleges körülmények (kritikusság, időbeli korlátok...)

RENDSZERLEÍRÁS

- A vizsgált rendszer leírása.
- Hol lett lefoglalva?
- Mire használják?
- Hogyan van konfigurálva (operációs rendszer, hálózat, perifériák)?
- Hogyan volt csatlakoztatva?
- Egyéb lényeges információ?
- Maga a rendszer és a környezet?

BIZONYÍTÉKOK MEGŐRZÉSE

A digitális bizonyítékok kezelésének teljes folyamatán keresztül fen kell tartani az információkat.

A cél a bizonyítékokra gyakorolt külső hatás minimalizálása és a befolyásolás elkerülése az alábbiak révén:

- A bizonyíték eltulajdonításától és manipulálástól való védelem.
- Az automatizált folyamatok (törlés, titkosítás) leállítása.
- Szükség esetén a bizalmas kezelés garantálása.

IGAZSÁGÜGYI SZAKVÉLEMÉNYEKKEL KAPCSOLATOS TIPIKUS HIBÁK

kompetencia megsértése

- jogkérdésben kinyilvánított vélemény
- kirendelő határozatban fel nem tett kérdésre adott válasz
- leleten kívüli forrásból származó bizonyítékra tekintettel adott szakvélemény

tartalmi megalapozatlanság

- iratellenesség
- téves következtetés
- hiányzó ténymegállapítás
- felderítetlenség

módszertani megalapozatlanság

- a szakértő nem, vagy értékelhetetlen sekélységgel jelöli meg a vizsgálati módszereket
- a szakértő nem, vagy értékelhetetlen sekélységgel jelöli meg a módszer validitását

HIBÁS SZAKVÉLEMÉNY

A sikeres jogorvoslat, kompenzáció gátja lehet a nem-megfelelő megközelítés, amelynek következményeként:

- nem gyűlik össze elegendő mennyiségű és/vagy minőségű bizonyíték,
- nem készül megfelelő dokumentáció a törvényszéki vizsgálatokról,
- a nyomkezelés nem megfelelősége miatt a vizsgálat nem megismételhető,
- hibák keletkeznek az elemzés vagy az értelmezés során.

KÖSZÖNÖM A FIGYELMET!

barkanyi.pal@kvk.uni-obuda.hu