VIZSGÁLATOK TECHNIKAI TÁMOGATÁSA

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Mai menü

- Bevezető
- „Forenzikus” rendszerek
- Begyűjtés
- Triage
- Labor
- Elvárások
- Paradigmaváltás

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Bevezető

Komáromi László

igazságügyi
informatikai biztonsági szakértő

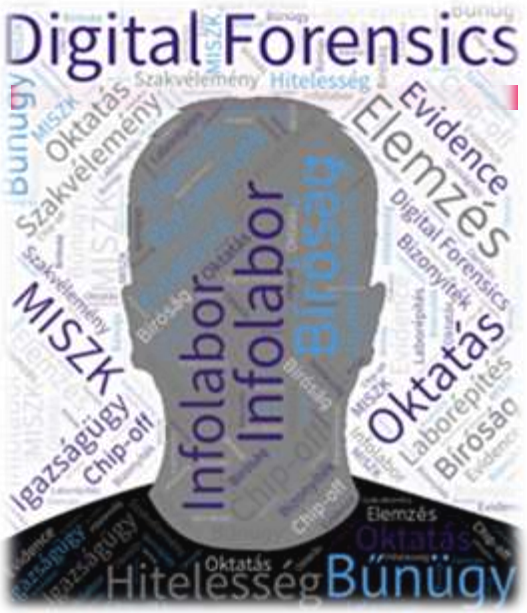
INFOLABOR
Infokommunikációs Szakértői Iroda Kft.

alapító-tulajdonos-ügyvezető

- RTF, BJKMF, ZMNE
  - Rendszerprogramozó, rendőrtiszt, biztonságtechnikai mérnök, védelmi informatikai rendszerszervező.

- 15 év rendőri szolgálat,
- 1 év bírósági adatvédelmi felelősi munka,
- 19 év igazságügyi informatikai szakértés.

- 1000+ szakértői ügy
- 100+ informatikai szakértői képzés
- 10+ szakértői labor építés



FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Bevezető

- Azonosítanak
- Megóvnak / megőriznek
- Összegyűjtenek
- Kinyernek
- Vizsgálnak
- Analizálnak
- Prezentálnak

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Forenzikus rendszerek

- Üzleti, vagy Open Source alapú megoldás;
- Célfejlesztés, vagy funkciók kihasználására épülő;
- Szoftver ÉS hardver együttműködő rendszere;
- Zárt, vagy OSINT / külső adatforrás bekötésű;
- Általánosan használt, vagy dedikált célterületre fejlesztett;
- Nyílt / korlátozott felhasználású,
  (szervezeti, territoriális, rendeltetési célú engedélyek).

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Forenzikus rendszerek

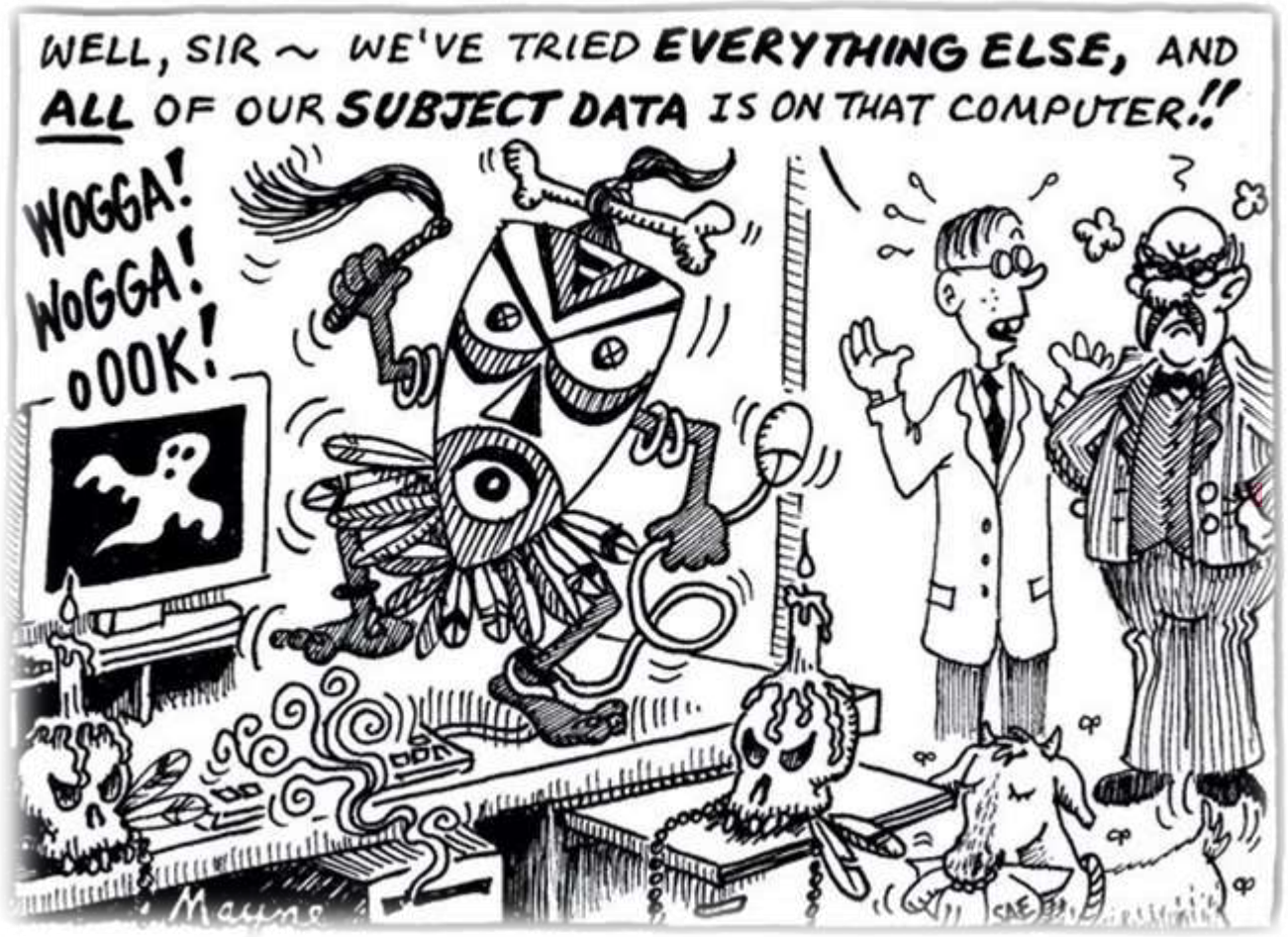
- Visszavezethető tevékenységi naplók;
- Hitelesített adatkezelési eljárások;
- Megfelelés a szakterület szabványainak;
- Megfelelés a best practice módszereknek;
- Megismételhető vagy reprodukálható vizsgálati eljárások;
- HASH, mint jellemzően kötelező elem…

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…

- AKKOR MOST MI MINDENT MENTÜNK!!!
- Ja, mégsem… HOGYAN ÉS MIT IS ADNAK ÁT?
- Hány gép / laptop / mobilkészülék?
- Mennyi háttértárra van szükségem?
- Megismételhető? Nem igazán!
- Ki fogja ezt feldolgozni?



FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…

WIEBETECH MOUSE JIGGLER

- Egyszerű, nem hagyja bekapcsolni a képernyővédőt…
- Működik Linux, Windows, MAC OSX felületen.
- Add oda a behatolóknak, hogy használják:
  IDŐT nyersz – TÖBBET, MINT GONDOLNÁD!

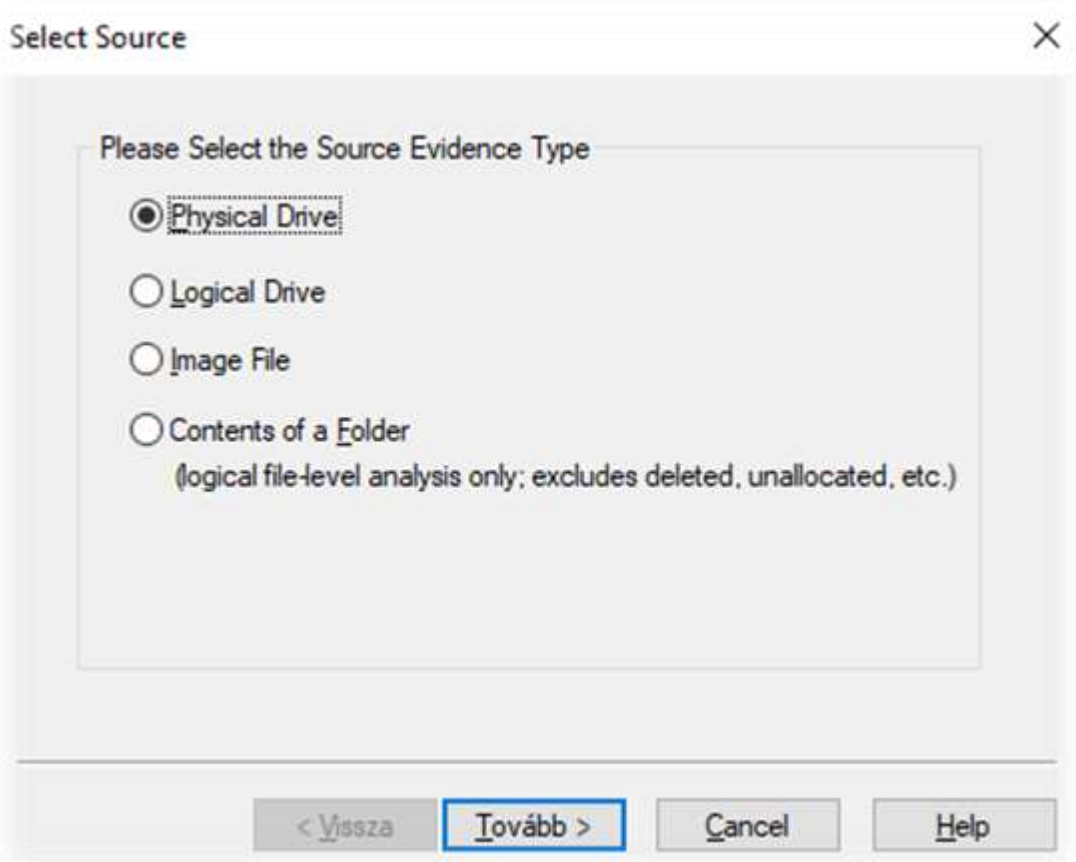
FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…

FTK IMAGER PORTABLE

- Svájci bicska!
- Másolat bármiről (kivéve mobilok!) amit háttértárként lát!
- Logikai / Fizikai image állományok készítése
- Portable: memory dump / REGISTRY!!!
- Standard formátumok!
- Írásvédő szükségeltetik!
- Később: Image Mounting!
- Free!?



FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…

IMAGER CÉLHARDVEREK

- Célirányos szoftver + hardver
- Gyors, zárt, elfogadott, kompatibilis.
- Logicube Falcon Neo: No1!!! – kiterjesztett lehetőségek…
- Opentext/Tableau TD4 – hát.. Nem igazán fejlesztik már…
- Wiebetech Ditto – ha csöndes megoldás kell…

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…

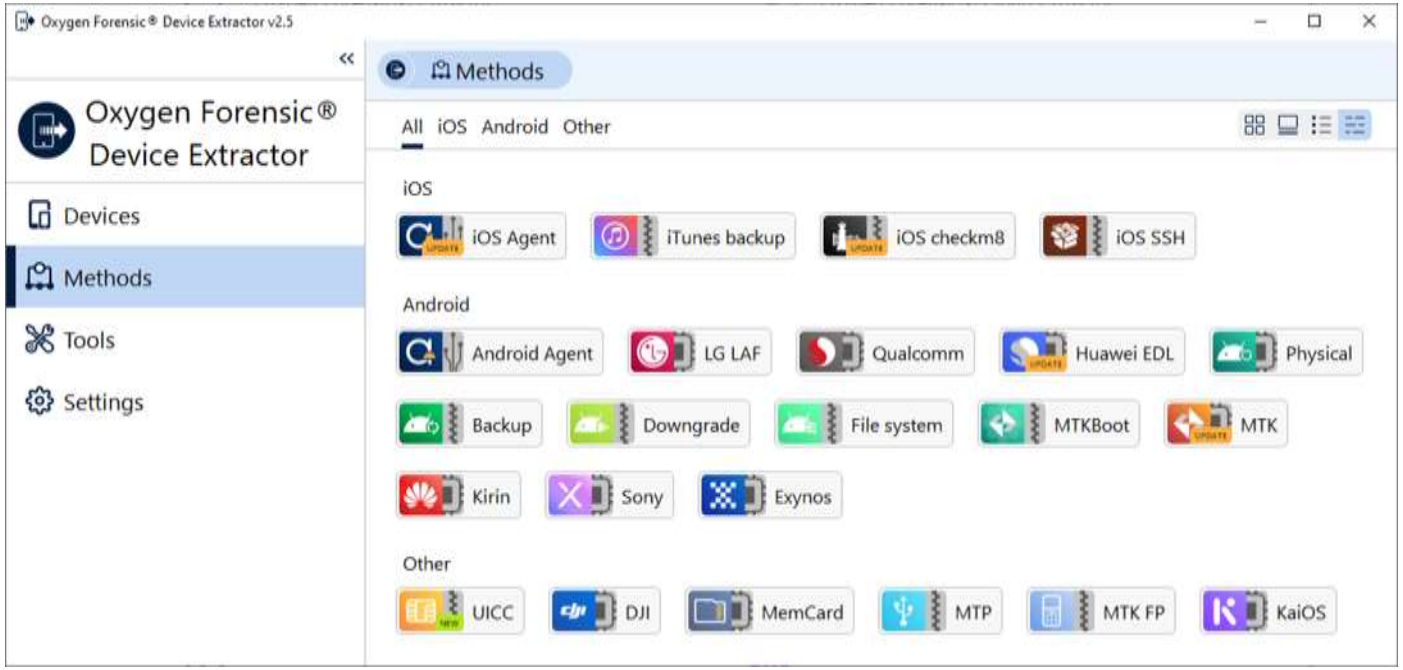
ÍRÁSVÉDŐK

- …mert muszáj megőrizni a sértetlenséget…
- NEHÉZ LENNE INDOKOLNI, HOGY MIÉRT NEM…
- Tableau – még mindig állja a helyét
- Logicube Portable Write Blocker
- Wiebetech Write Blocker USB
- Ha nincs más: Registry USB protect on/off

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A begyűjtés, vagy átadás…



MOBILESZKÖZÖKHÖZ

- Cellebrite termékek
- Oxygen Forensic Detective
- CFID

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Konszolidáció: Triage!

Nem szükséges mindent rögzíteni…

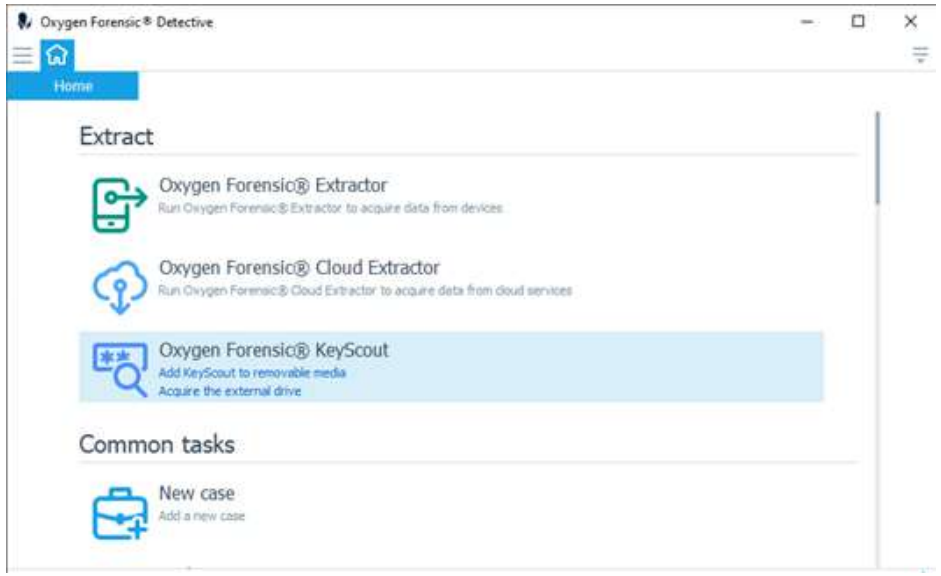
- Nincs IDŐ/ ERŐFORRÁS!
- Multihelyszín!
- Már tudjuk, hogy mit akarunk.
- Nincs szakértő akit helyszínre rakunk…
- Az ügygazda képzett!
- Kiválasztás!
- Döntöttek helyettünk…

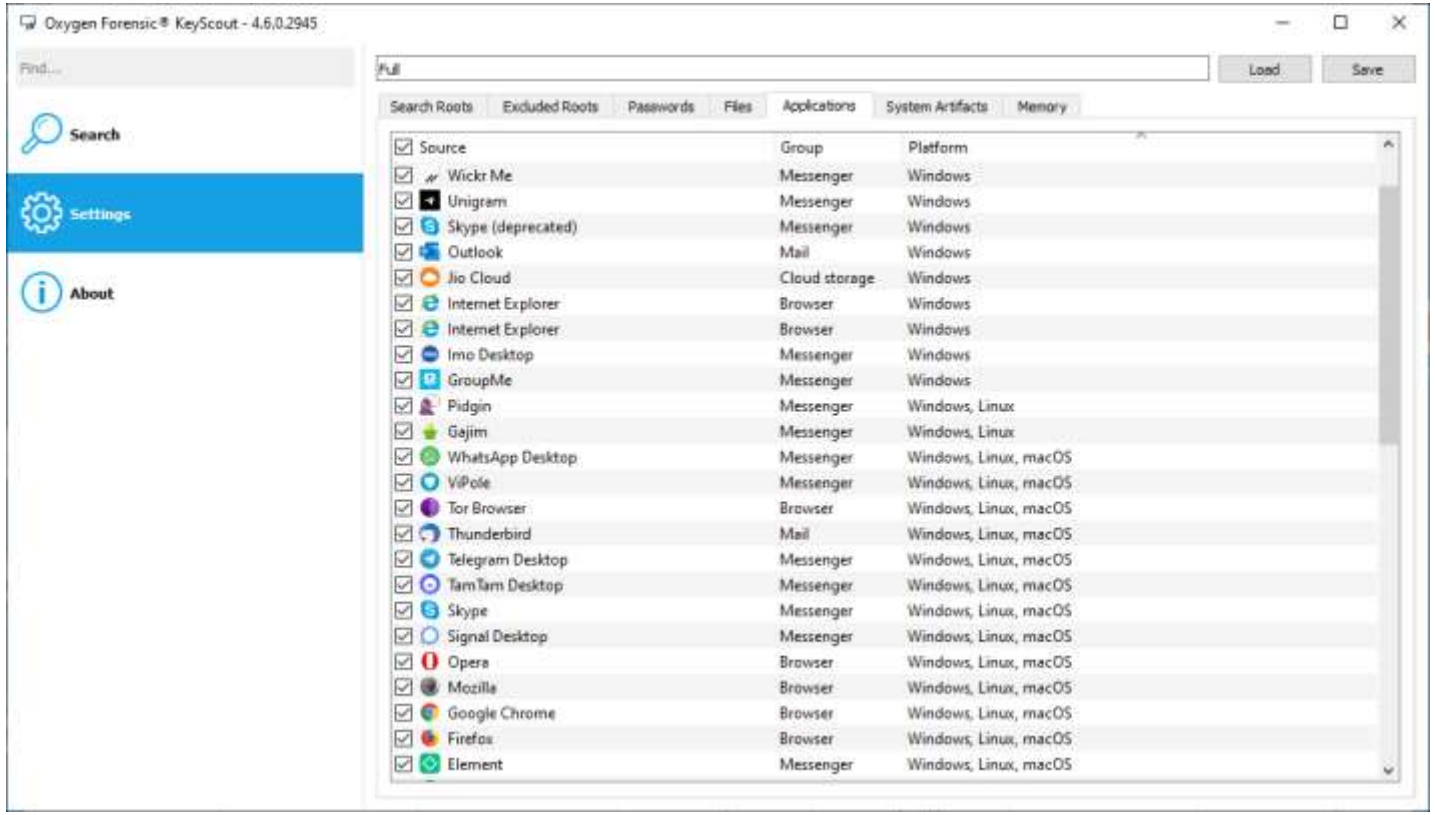
FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

Konszolidáció: Triage!

OXYGEN FORENSIC DETECTIVE - KEYSCOUT





FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor!

- Van időm…?!
- Szétszedéshez, kinyeréshez infók…
- Másolás/feldolgozás: éjszaka is megy…
- Telepített stabil és fix rendszerek.
- Nagyobb erőforrás áll rendelkezésre.
- Kialakított automatizmusok.
- Permanens információcsere az ügygazdával.
- Itt születik a riport!

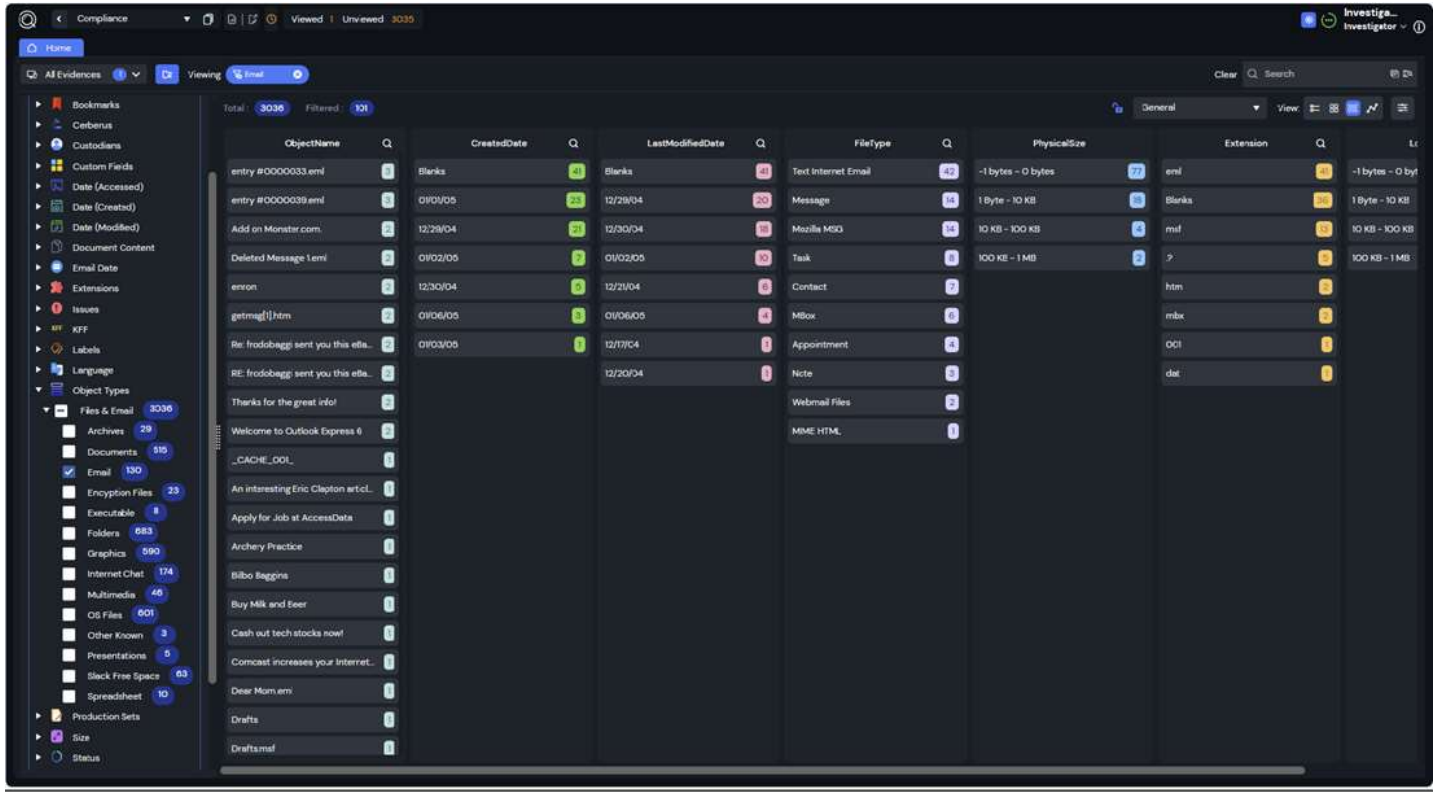
FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor!

EXTERRO FTK 8 – SMART VIEW

- Felhasználóbarát felület.
- Kategorizálás és szűrők.
- Idővonal alapú áttekintés.
- Mobiladatok feldolgozása.
- Automatizálható munkafolyamatok.
- Portable Case és FTK Connect.
- Riport és kereshető kivonat egyszerre!



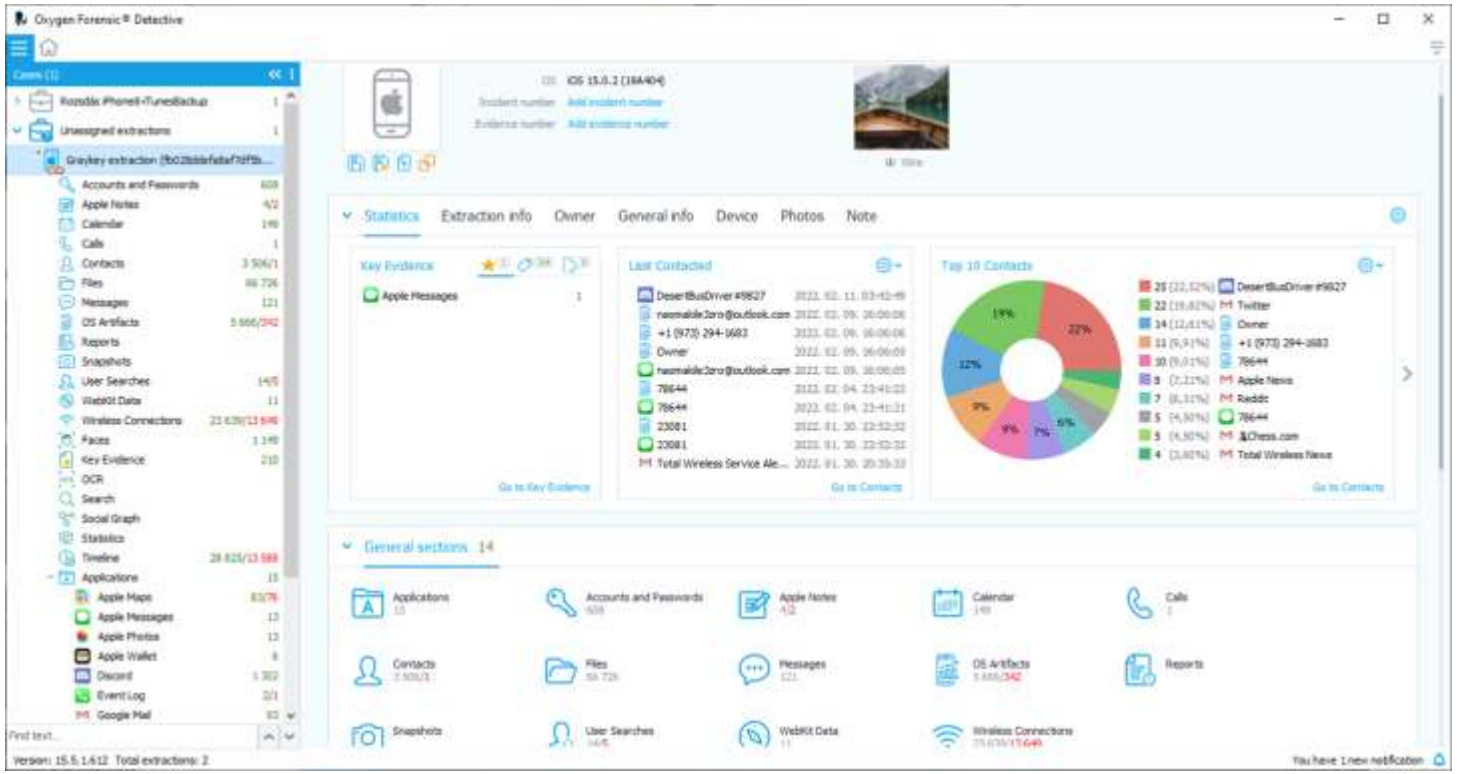
FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor!

OXYGEN FORENSIC DETECTIVE

- Mobilkészülékek letöltése.
- Több készülék adatainak összefésülése
- Importált (ADB, iTunes, ChipOff) adatok.
- Felhő alapú adattartalom kinyerés.
- Kapcsolati háló.
- KeyScout!
- Riport és kereshető kivonat egyszerre!



FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor – speciális eszközök

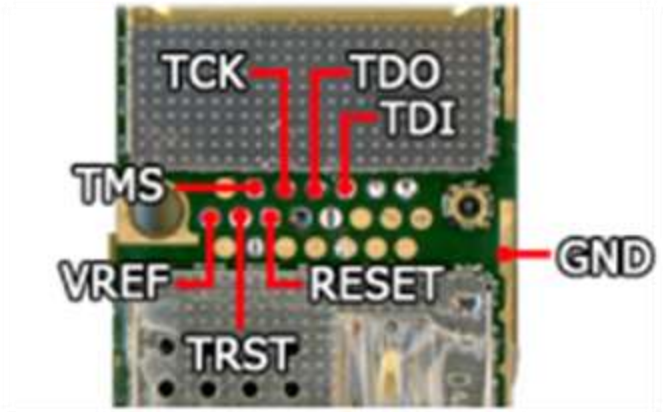
ACE Laboratory PC-3000 rendszerek

- Sérült adattárolók
- HD-Lock eltávolítás
- Törölt adattartalom speciális helyreállítása
- Invazív és Chip-off technikák támogatása

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor – speciális eszközök



Chip-off forensic munkaállomás

- Invazív technikák (JTAG, ISP, Chip-off)
- Sérült mobileszközök
- Sérült drónok

FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor – speciális eszközök

Jelszófeltörő rendszerek

- ElcomSoft, Passware, HashCat támogatás.
- GPU Rig-ek, vagy dedikált GPU szerverek.
- Elosztott rendszerek és agent alapú feldolgozás.
- Ha szenzitívek az adatok…

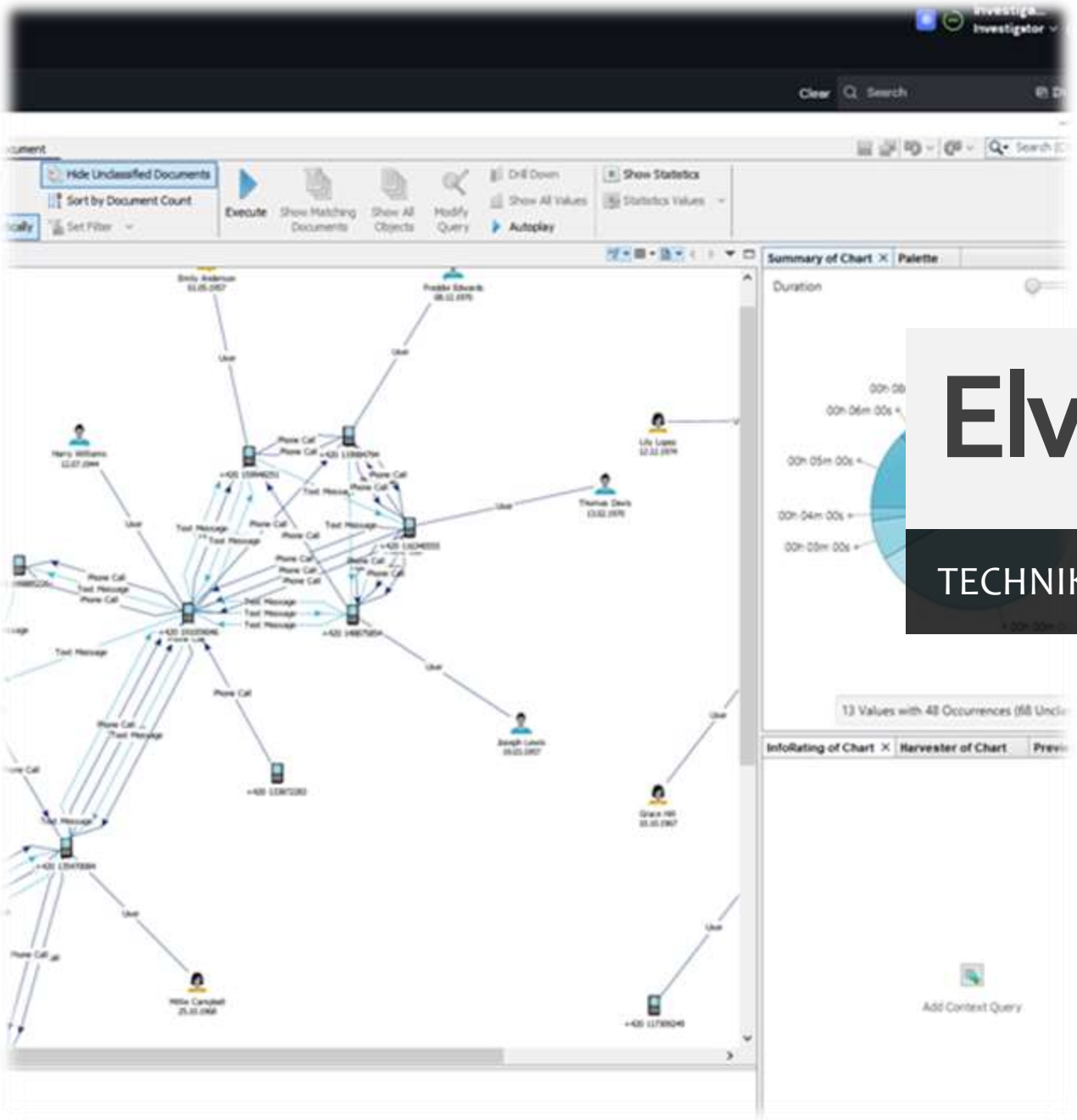
FORENSIC ESZKÖZÖK ÉS MÓDSZEREK

TECHNIKAI TÁMOGATÁS

A Labor – speciális eszközök

Háttértárak újra hasznosítása

- Felülírásos törlés.
- Napló és riportállomány.
- Többféle szabvány és eljárás támogatása.



Elvárások

TECHNIKAI TÁMOGATÁS

Hitelesség – Törvényesség - Relevancia

- Gyors és akkurátus feldolgozás.
- Célirányos, sallangmentes, érthető riportok.
- Lehetőség a további elemzésre.
- Dinamikus csapatmunka.

Technikai támogatás

PARADIGMAVÁLTÁS

Forensic paradigmák

- **Teljes másolat**
- **Hiteles adattartalom**
- **Egyszemélyes hadsereg (személyi felelősség)**
- **Területi hatály**
- **Offline és statikus rendszerekre kidolgozott metodikák**
- **Dogmatizált felhasználási területek – „A” hatóság!**

Átélt váltás: 2004-2008

Technikai támogatás

PARADIGMAVÁLTÁS

Katalizátorok?

- **Tárterületek extrém növekedése – Dawn Raid**
- **A Triage szemlélet egyre komfortosabb…**
- **„Munkaerő hiány” – a potenciált más terület szívja el**
- **„Mesterséges Intelligencián” alapuló feldolgozási mód**
- **Valós idejű és távoli rendszerek priorizációja**
- **Cyber, Compliance, GDPR – FORENSICALLY SOUND**
- **Fejlesztések: Enterprise orientáció - $$$**

VIZSGÁLATOK TECHNIKAI TÁMOGATÁSA

KÖSZÖNÖM A FIGYELMET!