

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszołgálati Egyetem
Rendészettudományi Kar

Számítógépek, laptopok közvetlen hozzáférésű memóriájának (RAM) forenzikus vizsgálata

Jelige: *Változékony valóság*

Pályamunka lezárásának időpontja: 2022. június

2023.

TARTALOMJEGYZÉK

1.	BEVEZETÉS	3
1.1.	A témaválasztásom indoklása.....	3
1.2.	A kutatásom hipotézisei.....	3
2.	A RAM MEMÓRIA TÖRTÉNETE, TULAJDONSÁGAI, JELENTŐSÉGE	5
2.1.	Történeti kitekintés és jellemzők	5
2.2.	A RAM memória jelentősége	7
3.	A HAZAI ÉS NEMZETKÖZI SZABÁLYOZÁS, SZAKMAI IRÁNYELVEK	11
3.1.	Nemzetközi szabályozás.....	14
4.	A MEMÓRIAMENTÉS ÉS ELEMZÉS GYAKORLATI ASPEKTUSAI	16
4.1.	A szemle	19
4.2.	A kutatás és lefoglalás	21
4.2.1.	A lefoglalás	24
5.	OPEN SOURCE ÉS KORLÁTOZOTT ELÉRÉSŰ SZOFTVEREK.....	27
5.1.	Zárt forráskódú alkalmazások	32
6.	ESETTANULMÁNY: BITLOCKER	43
7.	A JÖVŐ, LEHETSÉGES KIHÍVÁSOK.....	45
8.	ÖSSZEGZÉS, HIPOTÉZISEK IGAZOLÁSA	46
9.	ÁBRAJEGYZÉK	48
10.	IRODALOMJEGYZÉK.....	49
10.1.	Szakirodalmak	49
10.2.	Jogszabályok, rendeletek, módszertani levelek	50
10.3.	Előadások, konferenciák.....	51
10.4.	Internetes hivatkozások	51
11.	MELLÉKLETEK.....	53
11.1.	A teljes anonimizált esettanulmány	53
11.2.	Segédlet a számítógépek, laptopok közvetlen hozzáférésű memóriájának (RAM) lementéséhez és forenzikus vizsgálatához	56

1. BEVEZETÉS

1.1. A témaválasztásom indoklása

A témaválasztásom indítéka egészen az általános iskola első osztályáig vezethető vissza. Ebben az időszakban ismerkedtem meg a számítógéppel, mint számítástechnikai eszközzel. Igaz, ekkor még csak játszani tudtam rajtuk különféle számítógépes játékokkal. Az évek során fokozatosan kiismertem a különféle szoftvereket és algoritmusokat, amelyeknek köszönhetően sokoldalúbb informatikai tudásra tettem szert. A lelkesedésem az évek során sem hagyott alább.

Másrésről a bűncselekmények egyre nagyobb aránya valósul meg a kibertérben, illetve szinte minden büntetőeljárásban megjelennek az elektronikus adatok, mint bizonyítékok. A változékony adatok, melyek átmenetileg a RAM memóriában tárolódnak, sok esetben csak egyszeri alkalommal szerezhetők be a büntetőeljárások során, és ennek a jelentősége tette számomra fontossá a témakört, valamint annak kutatását. Ráadásul a 21. században a számítógépek és laptopok jelenléte olyan széles körben elterjedt, hogy közel minden háztartásban megtalálhatók. Ezt a folyamatot megerősítette a koronavírus járvány is, amely az otthoni munkára és a digitális oktatásra áttérés során még nagyobb szereppel ruházta fel a különféle elektronikus eszközöket.

A leendő Tudományos Diákköri Konferencia dolgozatomat, vagy szakdolgozatomat is kizárólag az informatikával, kiberbűnözéssel kapcsolatos témakörben tudtam volna elképzelni, amelyből úgy gondolom, hogy sikerült is egy számomra megfelelő témát találnom, a közvetlen hozzáférésű memória (későbbiekben RAM) forenzikus (bűnügyi/törvényszéki) vizsgálatát. A dolgozatomban kizárólag a személyi használatban lévő Windows, MAC OS X, Linux alapú számítógépek és laptopok kerülnek vizsgálat alá, mert Magyarországon napjainkban a személyi használatú eszközökön a különféle Windows változatok dominálnak, míg a Linux disztribúciók és a macOS változatok minimális mértékben, de jelen vannak.

1.2. A kutatásom hipotézisei

A dolgozatom megírása során az alábbi három feltételezésre kerestem igazolást a számítógépek, laptopok forenzikus vizsgálatának vonatkozásában.

1. Ahhoz, hogy egy memóriamentés és vizsgálat sikeresen végrehajtható legyen, a mentést végrehajtó személynek előzetes informatikai jártasságokra van szüksége, amely egy megfelelő mélységű oktatás és iránymutatás segítségével könnyedén elsajátíthatóvá válik.
2. Számos szoftvert kifejlesztettek már a memóriaképek elemzésére. Feltételezésem szerint az ingyenes, nyílt forráskódú szoftverek nem képesek olyan mélységben adatokat kinyerni a memóriafájlból, mint a hatóságok részére rendelkezésre álló, zárt forráskódú programok.
3. Nem állítható fel egyértelmű rangsor a memória elemzésének végrehajtása során az alkalmazott szoftverek között, köszönhetően a strukturális és megjelenési eltéréseknek. A nyomozó hatóságok által használt programok is rendelkezhetnek programozási hibával.

2. A RAM MEMÓRIA TÖRTÉNETE, TULAJDONSÁGAI, JELENTŐSÉGE

2.1. Történeti kitekintés és jellemzők

A számítógépek, laptopok, azon belül az alaplapok elengedhetetlen tartozéka a RAM memória. A RAM¹ (az angol Random Access Memory rövidítéseként: tetszőleges hozzáférésű memória, közvetlen hozzáférésű memória) egy véletlen elérésű írható-olvasható adattároló eszköz. Az elnevezés némileg félreérthető; a RAM memóriába nem tartozik bele a szintén véletlen elérésű, csak olvasható memória, a ROM. A memória kis bepattintható modulok formájában kapható és az alaplapok függvénye,² hogy hány darabot tudnak kezelni és milyen kapacitásig. A RAM tárolja a központi vezérlőegység (CPU) által végrehajtandó programokat, illetve a feldolgozásra váró adatokat. Az adatok, az éppen működő alkalmazások munkafolyamatai csak addig maradnak meg benne, amíg a számítógép feszültség, áramellátás alatt van, vagy ki nem lépünk a programból, ugyanis kikapcsoláskor, áramvesztéskor a benne tárolt adatok elvesznek. A gyorsítótár (cache) a memória modulon található és az a feladata, hogy kiegyenlítse a dinamikus RAM típusú áramkörök és a CPU regiszterei közötti sebességkülönbséget. Ennek módja az, hogy drágább, de gyorsabb statikus RAM cellákból alakítják ki a gyorsítótárat. A memória mérete meghatározza, hogy számítógépünk egyszerre hány alkalmazással és mennyi adattal tud dolgozni. A memória elérése nem véletlenszerűen, hanem pontos címzések alapján történik, az angol random szó itt arra utal, hogy egy adott memóriarész elérésének gyorsasága független az elhelyezkedésétől.³

A statikus RAM⁴ (Static Random Access Memory), vagyis statikus azonos elérési idejű tár celláinak jellemzője, hogy nem szükséges frissíteni annak tartalmát, mert a cellái billenő áramkörökből állnak. Az információt az áramvezetés iránya hordozza. Tulajdonságai miatt megfelelő volt a cache memóriaként történő alkalmazására. Hátránya, hogy nagy az energiafogyasztása és drága.

¹ Kibernetikázók kézikönyv. Szerk.: Nagy Zoltán András. Szerzők: Halász Viktor, Herédi István, Gyaraki Réka Kovács Zoltán, Máté István Zsolt, Nagy Zoltán András, Nagy Tamás, Simon Béla. In.: Ruzsonyi Péter (szerk.) – Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok, Ludovika Egyetemi Kiadó, 2020, 1783. oldal (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/TKP_Kozbiztonsag.pdf) Megtekintve: 2021.05.13.

² Fehér Krisztián: Számítógépvásárlási túlélőkönyv, szerzői magánkiadás, 2020, 14. o.

³ Mike Meyers: PC hardver és karbantartása, PANEM KFT, 2004, 87-116. o.

⁴ Máté István: A számítógép felépítése – Memóriák és csatlakozásuk. A BIOS., NSZFI, 2012, 6. oldal (https://www.academia.edu/1107969/Mem%C3%B3ri%C3%A1k_%C3%A9s_csatlakoztat%C3%A1suk_Working_with_computers_memory) Letöltve: 2021.11.02.

A dinamikus RAM⁵ (Dynamic Random Access Memory), vagyis dinamikus azonos elérési idejű tár kis előállítási költségeinek, valamint alacsony energiafelhasználási szintjükkel a 2000-es évek elején a leggyakrabban alkalmazták operatív tárként. Hátránya a lassú kiolvasási sebesség és a frissítések szükségessége.

A 2000-es évek elejétől az SDRAM (Synchronous dynamic random-access memory), azaz szinkron dinamikus közvetlen hozzáférésű memória vette át a szerepet a piacon egy rövidebb időre. Az SDRAM továbbfejlesztett kiadása a DDR SDRAM (Double Data Rate SDRAM), azaz dupla adatátviteli sebességű SDRAM volt. Napjainkban is ezek a RAM memória-fajták számítanak a legelterjedtebbnek, legnépszerűbbnek.

A DDR memória megjelenése 2000-es évek elején történt, az utolsó DRAM verziókkal párhuzamosan. Hozzávetőlegesen 200-400 MHz működési frekvenciával bírt. A DDR2 változat 2003-ban jelent meg, és 400-1066 MHz frekvenciára volt már képes. A 2007. évben megjelent DDR3 már 800MHz-től 2133 MHz, végül a 2014-től induló DDR4 nemzedék 1600 MHz működési frekvenciától használható. 2020-ban a kereskedelmi forgalomban kapható leggyorsabb DDR4-es memória 4600MHz működési frekvenciával bír.⁶ Manapság 4 GB méretű memória alatt nem érdemes vásárolni, mert a számítógép lassan fog vele dolgozni. Az operációs rendszer működése közben átlagosan 2 GB-ot foglal, ami ebben az esetben a memória felét jelentené, személyi használatú számítógépek, laptopok esetében 8 GB RAM-nál nagyobb kapacitás sem szükséges, amennyiben általános, hétköznapi feladatokra szeretnénk használni elektronikai eszközüket.

Ami a DDR memóriákat illeti, érdemes megemlíteni a GDDR3 (Graphics DDR3) típust. Ez a memóriaszabvány képes nagyobb sávszélességet biztosítani. Elsősorban grafikus kártyákon használják, amely csupán integrált formában érhető el. Szintén ugyanebben a formában elérhető el a GDDR5 memória, amelyet a grafikus kártyák mellett alkalmaznak még proceszorok mellett is olyan játékkonzolok esetében, mint a Playstation 4. A GDDR5 memória, modellektől és kiépítéstől függően, megközelítőleg 50-150 GByte/másodperc frissítési sebességre képes.

⁵ Máté István: A számítógép felépítése – Memóriák és csatlakozásuk. A BIOS. NSZFI, 2012, 5. oldal

⁶ Simon Béla – Kibernetika kézikönyv, Ludovika Egyetemi Kiadó, 2020. 1783. o.

Napjainkban a DDR3 és DDR4 memóriatípusok a legelterjedtebbek, de még ebben az évben piacra fog kerülni a DDR5-ös változat. Az általános célú személyi számítógépek, laptopok konfigurációjába indokolt legalább 8 GB RAM elhelyezése a növekvő hardverigények ki-elégítése és a felhasználói élmény csökkenésének elkerülése végett.

2.2. A RAM memória jelentősége

A RAM memóriát, más néven az operatív tárat vagy fő memóriát (main memory), egészen a 2000-es évek elejéig nem tartották releváns bizonyítékforrásnak. Ez a megállapítás 2005-ben kezdett megváltozni, amikor megtartották az Digital Forensic Research Workshop konferenciát,⁷ melynek egyik kérdésköre a memória elemzése volt és egy feladatot (kihívást) tartalmazott. Ennek eredményeképpen Microsoft Windows alapú operációs rendszerekre kifejlesztettek számos memóriaelemző eszközt, mint például a „memparser” és a „kntlist”. Mivel jelentős fejlődés ment végbe a Windows rendszerek tekintetében, ezért szükség volt a kutatási törekvéseket a Linux memóriaelemző szoftverek fejlesztésére összpontosítani. A Digital Forensic Research Workshop 2008-as Kihívás⁸ tanácskozása már nemcsak a Linux operációs rendszerre, hanem az egyéb forrásból származó bizonyítékok integrálására összpontosított.

Az évek során Digital Forensic Research Workshop tanácskozásainak alapvető szerepe volt a RAM memória adattartamának és a benne tárolt digitális bizonyítékok felértékelődésében. Kriminálisztikai és eljárásjogi szempontból a történeti tényállás felderítéséhez szükséges a tárgyi, illetve személyi bizonyítékokat felderíteni, összegyűjteni, amelyeknek köszönhetően megalapozható lesz az elkövető büntetőjogi felelőssége. A felderített elektronikus bizonyítékokat a törvényesség elvének megfelelően kell rögzíteni, megőrzéséről pedig úgy szükséges gondoskodni, hogy az később az eljárás során bármikor felhasználhatók legyenek. A közvetlen memóriából történő adatrögzítés során a tárgyi bizonyítékok olyan adatok, amelyek a digitális térben keletkeztek, és a memória, mint adathordozó tárolja. Megszerzése olyan bizonyítási cselekmények és kényszerintézkedések keretein belül történik, mint a szemle, kutatás, lefoglalás. Elemzése pedig laboratóriumi körülmények között, az eljáró szervnél történik. Helyszínen történő bűnügyi adatmentés során a RAM memóriából igyekeznek a lehető legtöbb releváns információt kinyerni az erre programozott célszoftverekkel. Jelen esetben a hatósági adatmentés

⁷ DFRWS. DFRWS 2005 forensics challenge, 2005. <http://old.dfrws.org/2005/challenge/index.shtml> (Letöltés ideje: 2021.05.12.)

⁸ Geiger, M., Venema, W., and Casey, E. DFRWS 2008 forensics challenge, 2008 <http://old.dfrws.org/2008/challenge/index.shtml> (Letöltés ideje: 2021.05.12.)

indokoltságát az adja, hogy nem tűr halasztást a memória által tárolt adatok beszerzése. Egy bekapcsolással vagy kikapcsolással már elveszti az adattartalmát. A számítástechnikában az igazságügyi elemzéseket általában „in vivo” és „post mortem” kategóriákba sorolják.⁹ Az „in vivo” kifejezés a futó és reagáló rendszer elemzésével, a „post mortem” pedig már a kikapcsolt állapotú, korábban összegyűjtött adatok elemzésével fordítható.

Egy futó számítógépnek vagy laptopnak a pillanatnyi memóriájában számos digitális adat lelhető fel, amely egy eljárás során fontos tárgyi bizonyítási eszközként is szerepelhet. A 2017. évi XC törvény (a továbbiakban: Be.) szerint tárgyi bizonyítási eszköz minden olyan tárgy – ideértve az iratot és az okiratot is –, amely a bizonyítandó tény bizonyítására alkalmas, így különösen az, amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza, amely a bűncselekmény elkövetése útján jött létre, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amelyre a bűncselekményt elkövették.¹⁰

A törvényi hivatkozás az irat fogalma szerint nyer értelmezést, miszerint irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít, így különösen a papíralapú vagy elektronikus adatként létező szöveg, rajz, ábra.¹¹ Amíg az 1998. évi XIX. törvény¹² (a továbbiakban: régi Be.) az elektronikus adat hordozója tárgyi bizonyítási eszköznek számít, úgy az új, 2017-es büntetőeljárásról törvény az elektronikus adatot¹³ is a bizonyítás eszközeinek sorolja, lépést tartva jogalkotói szinten a számítástechnikai fejlődéssel.

Egy RAM memória adattartalma böngészési előzményeket, elektronikus levelezési (a továbbiakban: e-mail) fiókok, fájlok, tevékenységi előzmények, IP-címek, Facebook fiókok, jel-szavak, illetve kártékony programok kódjait is tartalmazhatja. A felsorolt elektronikus adatok elemzése igazságügyi informatikai szakértői kompetencia, de előfordulnak olyan esetek, amikor a nyomozó hatóság végzi pl.: a mobilkommunikációs eszközök kivonatolása.

⁹ Ivor Kollár: Forensic RAM dump image analyser, Univerzita Karlova, 2010, 6-7. o.

https://dspace.cuni.cz/bitstream/handle/20.500.11956/34206/DPTX_2007_1_11320_0_231778_0_48540.pdf?sequence=1&isAllowed=y (Letöltés ideje: 2021.05.13.)

¹⁰ 2017. évi XC. törvény a büntetőeljárásról (a továbbiakban: Be.) 204. § (1) bek. (<https://njt.hu/jogszabaly/2017-90-00-00>) Megtekintve: 2021.09.28.

¹¹ Be. törvény 204. § (2) bek.

¹² 1998. évi XIX. törvény a büntetőeljárásról (<https://njt.hu/jogszabaly/1998-19-00-00>) Megtekintve: 2021.10.08.

¹³ Be. 165. § f) pontja

A kártékony programok, azaz malware-ek (angolul malicious software) rosszindulatú szoftverek összevonásából kialakított mozaikszó,¹⁴ amely magába foglalja a vírusokat, kémprogramokat, trójai vírusokat, valamint agresszív reklámprogramokat. Munkavállalók, illetve magánfelhasználók bizonyos feltételek teljesülése esetén egyaránt válhatnak malware-támadás áldozatává. Ehhez elegendő egy hamis e-mail-en belüli hivatkozásra kattintanunk, nem megfelelő alkalmazást letöltenünk, valamint rosszabb esetben banki és személyes adatainkat is megszerezhetik akár álweboldalak használatával. Bizonyos kártékony kódok kizárólag a RAM memóriaképből olvashatók ki. Ezek mélyen rejtőznek egy számítógépben vagy laptopban, és képesek a készüléket használó magánszemély vagy munkavállaló észrevétele nélkül átvenni az irányítást a számítástechnikai eszköz felett egy másik, illetéktelen felhasználó által.

A memóriamentési folyamat megkezdése előtt fontosnak tartom megemlíteni, hogy amennyiben rendelkezünk nem saját felhasználású, hanem nyomozó hatóság által biztosított USB adathordozóval, DVD-vel, külső merevlemezzel úgy a bűnügyi technikus, vagy akár a nyomozó hatóságok tagjai is végre tudják hajtani a memóriamentést, amennyiben rendelkeznek erre vonatkozó kiképzéssel, mivel egyszerűbb és rövidebb folyamatnak tekinthető a memória elemzéséhez képest. Egy pendrive, esetleg külső merevlemez alkalmazása sokkal előnyösebb, mint DVD-t applikálni, mert megváltoztatható adathordozók, nagyobb kapacitással rendelkeznek, és nem kell lemezíró alkalmazás a használatukhoz. Az elemzéshez célszerű szakértőt kirendelni, mert az eredményes lefolytatás különös szakértelmet igényel.

A memóriáról hiteles igazságügyi másolat manapság certifikációval ellátott és nyílt forráskódú memóriakép készítésére alkalmas szoftverrel hozható létre, amelyeket az igazságszolgáltatás elfogad. Erre egy jó példa az Exterro megnevezésű vállalat forenzikus lemezképkészítő szoftvere, az Accesdata Forensic Toolkit Imager¹⁵ (a továbbiakban: FTK Imager), de ilyen szoftver többek között a WinPmem,¹⁶ amelyeknek a 32 és 64 bites verziója is elérhető. Vassil Roussev professzor szerint¹⁷ a memóriaelemzés kétféleképpen valósítható meg, nevezetesen egy élő (futó) rendszeren (angol szaknyelven live analysis), vagy a rendszermemória állapotának pillanatképén (snapshot). A RAM memória rögzítése során egy memóriakép keletkezik,

¹⁴ Nagy Zoltán: A kiberbűncselekmények fogalma és csoportosítása, In.: Kiss Tibor – Kibervédelem a bűnügyi tudományokban, dialóg campus, Budapest, 2020, 37. o. (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf) Letöltve: 2021.10.12.

¹⁵ Accesdata Forensic Toolkit (továbbiakban: FTK) Imager (<https://accessdata.com/product-download/ftk-imager-version-4-5>) Megtekintve: 2021.09.28.

¹⁶ WinPmem (<https://github.com/Velocidex/WinPmem>) Megtekintve: 2021.09.28.

¹⁷ Vassil Roussev: Digital Forensic Science: Issues, Methods, and Challenges, University of New Orleans 2017, 63. o.

nevezetesen egy .mem fájl. Ennek eredménye az operatív tár pillanatnyi adattartalmáról készített memóriakép állomány.¹⁸

Mivel másolási folyamatról beszélünk, ezért az eredeti adatok állapota nem változik meg. A másolatkészítésnek három típusa van, nevezetesen teljes bitazonos másolat, forenzikus másolat, egyszerű másolat. A RAM memória esetében, mivel élő rendszer elemzéséről (live analysis) van szó, a benne tárolt elektronikus adatok még a memóriamentési folyamat során is változnak, ezért nem képezhető le az adathordozóról minden bitre megegyező másolat. Hiteles/forenzikus másolat (angol szaknyelven *forensic clone*) viszont igen. Ilyenkor egy úgynevezett konténer-fájlba tömörítik a kinyert memóriamásolatokat, így kevesebb tárhelyet vesz igénybe a tömörített adatösszesség, mint az eredeti, az adattartalma viszont nem változik. A kiterjesztésnek AccessData 1 a megnevezése (AD1), mely egyéni tartalmú lemezképek létrehozásánál használnak. Ennek eredményeképpen kétszer vagy többször ugyanabban a formátumban sem menthető le a RAM. A hash-kulcsnak köszönhetően viszont biztosítható, amit automatikusan kikalkulál az FTK Imager, hogy a lefoglaláskori és a vizsgált adatállomány integritása bármikor igazolható legyen.

¹⁸ A Magyar igazságügyi Szakértői Kamara (a továbbiakban: MISZK) 6/2020 Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről, 2020, 25. oldal (https://misk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf) Letöltés ideje: 2021.08.24.

3. A HAZAI ÉS NEMZETKÖZI SZABÁLYOZÁS, SZAKMAI IRÁNYELVEK

Hazánkban jelenleg nincs számítógépes bűncselekményekkel kapcsolatos, különálló anyagi- és eljárásjogi szabályozás. A normatív szabályozás hiányának köszönhetően nincs tudományosan, széles körben elfogadott egységes meghatározás. Ebben az esetben az általánosan érvényben lévő szabályokat kell alkalmazni. Az eljáró hatóságoknak a kényszerintézkedések, illetve egyéb eljárási cselekmények törvényi ismerete mellett az egyéni problémamegoldó készségüket, kreativitásukat is alkalmazniuk kell olyan eljárásjogi alapelvek mentén, mint a törvényesség, arányosság, egyenlőség, eredményesség. A kibertérben vagy bármilyen, informatikai eszközökkel vagy eszköz/rendszer ellen elkövetett jogellenes cselekmény esetében is a büntetőeljárásról szóló törvény rendelkezéseit kell alkalmazni.¹⁹ Útmutatóként szolgálnak továbbá a kormányrendeletek, rendeletek, módszertani levelek és a kapitányságok belső dokumentumai, előadásai.

A régi Be. törvényben (1998. évi XIX. törvény) még nem volt megfogalmazva az információs rendszer, illetve az adathordozó átvizsgálása. A számítástechnikai eszközök adattartalmának beszerzését és felhasználását a gyakorlat formálta. A rögzített elektronikus adatot a rendőrség által biztosított adathordozóval együtt egységesen foglalták le. Az adat helyett az adathordozó került bűnjelezésre, amelyből folyamatosan kellett új darabokat beszerezni, és tárhelyük kihasználtsága minimum szinten mozgott. Az új büntetőeljárásról szóló törvényben már történtek érdemi változások. Jogilag legitimálja a számítógépek, laptopok forenzikus célú vizsgálatát. Megbontotta az adat és adathordozó lefoglalásának egységét, amely egy fontos előrelépésnek tekinthető. Az elektronikus adat, mint bizonyítási eszköz ezzel a rendelkezéssel ugyan korlátozottabb formában, de felkutathatóvá, rögzíthetővé vált, és az eljárási cselekmények vonatkozásában jelentős tárgyi bizonyítási szerepet képviselhet. A gyakorlatban természetesen még manapság is van, aki a régi, megszokott módszert alkalmazza feleslegesen. Ami a beszerzendő információt illeti, a helyszínen történő lefoglalása abban az esetekben valósulhat meg, ha az kiemelt fontossággal bír, kinyeréséhez speciális szakértelem szükséges, illetve tartani lehet attól, hogy felülírják, esetleg törlik az adatokat. Ez magyarázza a kutatáshoz szorosan kapcsolódó lefoglalás kényszerintézkedést.

¹⁹ Gyarakí Réka – Simon Béla: Kiberbűncselekmények felderítése és nyomozása, 124. o. In.: Kiss Tibor – Kibervédelem a bünygyi tudományokban, Dialóg Campus, Budapest, 2020. (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf) Letölt ideje: 2021.06.08.

„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”²⁰ Az elektronikus adat, mint normatív, jogszabályban rögzített definíció már a régi büntetőeljárási törvényhez képest is fontos mérőöldkőnek számított, hiszen a technológiai fejlődéssel párhuzamosan egyre nagyobb szükség volt a jogalkotó általi szabályozásra. Emellett főszabály szerint ahol a Be. törvény tárgyi bizonyítási eszközt említ, eltérő rendelkezés hiányában az elektronikus adatot,²¹ mint sajátos formát kell érteni.

A 100/2018 (VI.8.) Korm. rendelet²² (továbbiakban: Nyer) a nyomozás és az előkészítő eljárás részletes szabályairól, mint végrehajtási rendelet számottevő rendelkezéseket foglal magába az elektronikus adat vonatkozásában, a szaktanácsadó igénybevételéről és az eljárási cselekmény lefolytatásának részletes szabályairól.

A 11/2003. (V.8.) IM-BM-PM²³ együttes rendelet az elektronikus adatokra vonatkozóan tartalmaz további rendelkezéseket. Részletezi, hogy az elektronikus adat lefoglalását hogyan kell végrehajtani, útmutatást ad a dokumentálására, valamint megszabja, mikor melyik típusát kell alkalmazni a lefoglalásnak a Be. 315 § (1) bekezdés felsorolásából. Megemlíti, hogy az adatmentésre használt adathordozó előzetesen ne tartalmazzon adatokat, illetve a másolt adattárolmány utólagos megváltoztatását is kerülni kell, vagy megváltoztatás esetén nyomon követhetően, részletesen dokumentálva legyen. A jegyzőkönyvben kötelező rögzíteni a másoláshoz használt adathordozó típusát, gyártási számát, a rajta tárolt adat jellegét és tartalmát, megkönynyítve ezzel a későbbiekben az adat nyomonkövethetőségét a rendőrségen belül. Az új büntetőeljárási törvény és a bűnjelkezelésről szóló rendelet módosításának köszönhetően manapság az elektronikus adatok lefoglalásának, kezelésének szabályozása alkalmassá vált a napjainkban kialakult digitális követelmények teljesítésére.

A Magyar Igazságügyi Szakértői Kamara (a továbbiakban: MISZK) 6/2020. számú Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről²⁴ megfogalmaz olyan esszenciális lépéseket, amelyeket a helyszíni adatmentés előtt elengedhetetlen teljesíteni. A

²⁰ Be. törvény 205. § (1) bek.

²¹ Be. 205. § (2) bek.

²² 100/2018. (VI. 8.) Korm. rendelet (továbbiakban: Nyer) (<https://njt.hu/jogszabaly/2018-100-20-22>) Letöltés ideje: 2021.09.07.

²³ 11/2003 (V.8.) IM-BM-PM együttes rendelet 67. § (<https://njt.hu/jogszabaly/2003-11-20-06>) [2021.09.14.]

²⁴ MISZK 6/2020 Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről (https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf) Megtekintve: 2021.09.20–.

Módszertani levél kiadásáról az elnökség döntött az igazságügyi szakértői tevékenység egységes és magas színvonalú ellátása érdekében.²⁵ Ennek köszönhetően egy egységes írás áll rendelkezésre annak érdekében, hogy miként szükséges felkészülni egy külső helyszínen történő adatmentésre, majd a labor körülmények közötti elemzésre. A memóriakép, mint az igazságügyi másolat egyik fajtája, annak rögzítésével és elemzésével kapcsolatban a kamara módszertani levele is tartalmaz rendelkezéseket.

Ami az igazságügyi informatikai szakértőket és szaktanácsadókat illeti, mivel a személyi számítógépeken, laptopokon található digitális adatok helyszínen történő rögzítése elsősorban informatikai szakértői vagy szaktanácsadói kompetencia,²⁶ úgy az igazságügyi informatikai szakértő feladatát a 2016. évi XXIX. törvény az igazságügyi informatikai szakértőkről, a 9/2006. (II.27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről, a MISZK 6/2020 számú módszertani levele és az új Be. törvény rendelkezései a meghatározóak. Kirendelésük szakértő kirendelő határozattal történik. A szaktanácsadókra többek között a Nyer. tartalmaz rendelkezéseket.

A lefoglalás során a Be. törvény egyértelműen felsorolja a lefoglalható dolgok körét, többek között az elektronikus adat lefoglalását.²⁷ A végrehajtás módja a digitális adat vonatkozásában történhet másolat készítésével, áthelyezéssel, az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy jogszabályban meghatározott más módon. Egyetlen opció kimaradt, amely RAM memória esetében releváns és alkalmazandó, mégpedig az adathordozó teljes tartalmáról történő másolat készítésével végrehajtott lefoglalás. A 11/2003. (V.8.) IM-BM-PM együttes rendelet alapján akkor van erre lehetőség, ha az információs rendszer vagy adathordozó teljes adattartalmának lényege van, illetve a bizonyítás érdekében előre meg nem határozható, vagy jelentős mennyiségű adat átvizsgálására van szükség.²⁸

A hazai hatásköri és illetékességi kérdésről a 25/2013. (VI.24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről tartalmazza a jogszabályi háttérrel az büntetőeljárás lefolytatására. Alapesetben tehát az a nyomozó hatóság jogosult a nyomozás lefolytatására, amelynek illetékességi területén – sorozatbűncselekmények esetén a bűncselekmények többségét – elkövették.²⁹ Természetesen a rendelet kitér a hatásköri vagy illetékességi

²⁵ 2016. évi XXIX. törvény az igazságügyi szakértőkről 89. § (1) bek. (<https://njt.hu/jogszabaly/2016-29-00-00>) Megtekintve: 2021.09.20.

²⁶ Anti Csaba László, Gárdonyi Gergely: Krimináltechnikai Kézikönyv - Módszertani útmutató bűnügyi technikusoknak 2., Semmelweis Kiadó, 2020, 7. fejezet, 231. o.

²⁷ Be. 315. § (1) bek.

²⁸ 11/2003 (V.8.) IM-BM-PM együttes rendelet 67 § (4) bek.

²⁹ 25/2013. (VI.24.) BM rendelet 3. § (1) bek. (<https://njt.hu/jogszabaly/2013-25-20-0A>) [2021.09.20.]

vita esetén is az eljárási folyamatra, illetve a halaszthatatlan nyomozási cselekmények lebonyolítására.

A Be. 315 § (4) bekezdése alapján az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse. Egy adathordozónál, különösen a közvetlen memória esetében, nem lehet az arányosság elvét szem előtt tartani, hiszen a benne tárolt elektronikus adatok mennyisége előre meg nem határozható, jelentős mennyiségű, amelynek átvizsgálása szükségszerű a büntetőeljárás szempontjából.

3.1. Nemzetközi szabályozás

Ami a kiberbűncselekmények nemzetközi anyagi jogi szabályozását illeti, napjainkban az Egyesült Államok bizonyos tagállamaiban már megfogalmaztak a számítógépes bűncselekményekkel kapcsolatos egységes anyagi és eljárásjogi szabályozást. Erre egy jó példa Észak-Karolina számítógépes bűnözéssel kapcsolatos törvénye, a 2010 North Carolina Code Chapter 14 Criminal Law, Article 60 – Computer Related Crime.³⁰ A törvényben ténylegesen részletezik az egyes bűncselekmények definícióit, az egyes bűncselekmények megvalósulásának követelményeit, hatásköri és illetékességi felosztását, valamint a kiszabható büntetések kategóriáját és mértékét.

Az Európa Tanács már 2001. november 23-án megalkotta Számítástechnikai Bűnözésről szóló Egyezményt, amikor Budapesten ülésezett. Ennek köszönhetően nevezik ezt a nemzetközi okmányt budapesti egyezménynek. Magyarországon a 2004. évi LXXIX törvénnyel hirdette ki az országgyűlés az uniós jogszabályt. Ennek következtében a 2012. évi C. törvény a Büntető Törvénykönyvről³¹ is kiegészült a nemzetközi jog egyes rendelkezéseivel. Olyan meghatározások kerültek egységes törvényi környezetbe, mint a számítástechnikai rendszer, a szolgáltató, forgalmi adat.³² Az első fejezetében anyagi jogi, a második fejezetében büntető eljárásjogi, a harmadikban pedig joghatósági rendelkezéseket tartalmaz az Egyezmény, amely egy új mérőföldkőnek számított a nemzetközi jogi szabályozásra vonatkozóan. Eljárásjogi szempontból olyan irányelvek kerültek beemelésre a jogrendszerünkbe, mint a rendelkezések alkalmazási

³⁰ Észak-Karolina számítógépes bűnözéssel kapcsolatos törvénye (<https://law.justia.com/codes/north-carolina/2010/chapter14/article60/>) Megtekintve: 2021.09.20.

³¹ 2012. évi C törvény a Büntető Törvénykönyvről (<https://njt.hu/jogszabaly/2012-100-00-00>) [2021.10.09.]

³² 2004. évi LXXIX törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (<https://njt.hu/jogszabaly/2004-79-00-00>) [2021.09.21.]

köre, a garanciák és biztosítékok, a közlésre kötelezés, valamint a tárolt számítástechnikai adatok átvizsgálása és lefoglalása, többek között másolat készítésével. Egy olyan alapot adott a kiberbűncselekmények szabályozásához, hogy az új nemzetközi kezdeményezések általában erre épülnek. 2003-ban kiegészítették az Egyezményt, de egyes bűncselekmények szabályozását még így sem foglalja magába.

Az Európa Parlament és a Tanács 2013. augusztus 12-én kiadta a 2013/40/ EU irányelvet³³ az információs rendszerek elleni támadásokról. Megfogalmazásra kerültek a számítógépes bűncselekményekkel kapcsolatos tényállások, a szankciók és jogkövetkezmények minimumszintje, és az illetékes hatóságok, valamint az Európai Unió ügynökségei és szervei közötti hatékony együttműködés előmozdítása. Az új előírásoknak köszönhetően számos új kiberbűncselekmény törvényi tényállása és szankcionálása került beemelésre. A nemzetközi irányelvet a tagállamoknak 2015. szeptember 4-ig kellett implementálniuk a nemzeti jogukba.³⁴

Végül, de nem utolsósorban, néhány nemzetközi szervezet szabványai releváns ajánlásokat fogalmaznak meg a digitális adatok, bizonyítékok vonatkozásában, azok összegyűjtéséhez, megszerzéséhez, elemzéséhez. Ide tartozik a Digitális Bizonyítékokkal Foglalkozó Tudományos Munkacsoport (Scientific Working Group on Digital Evidence)³⁵, az Európai Forenzikus Szakértői Intézetek Hálózata (European Network of Forensic Science Institutes)³⁶, és az Európai Unió Hálózat- és Információbiztonsági Ügynökség (European Union Agency for Cybersecurity)³⁷ szervezete. Az említett szervezetek számos irányelveit építették bele a hazai MISZK 6/2020-as Módszertani levelébe.

³³ Az Európai parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról, (1) bek. (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32013L0040>) Megtekintve: 2021.09.21.

³⁴ Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények egyetemi jegyzet, Pécs, 2017, 88. o.

³⁵ SWGDE (<https://www.swgde.org/>) Megtekintve: 2021.10.08.

³⁶ ENFSI (<https://enfsi.eu/>) Megtekintve: 2021.10.08.

³⁷ ENISA (<https://www.enisa.europa.eu/>) Megtekintve: 2021.10.08.

4. A MEMÓRIAMENTÉS ÉS ELEMZÉS GYAKORLATI ASPEKTUSAI

A személyi számítógépek nyomozó hatóság általi észlelése, felismerése az esetek döntő többségében nem okozhat komolyabb fejtörést. Általában álló gépházak a gyakoriak, hozzájuk tartozik a monitor és egyéb perifériák, mint billentyűzet, egér, hangszóró. A hordozható számítógépek, azaz laptopok nevéből kifolyólag a könnyű helyváltoztatás miatt különbözik a személyi számítógépektől. Beépített kijelzővel és billentyűzettel rendelkeznek. Az említett elektronikus eszközökön található digitális adatok helyszínen történő rögzítése általában olyan bizonyítási cselekmények és kényszerintézkedések keretein belül kerül foganatosításra, mint a szemle, a kutatás és lefoglalás. Adatkéréssel elméletben megvalósítható az operatív tár adattartalmának rögzítése, viszont az eljárás során mindenféleképpen szükséges az adathordozó szakértő vagy a nyomozó hatóság által mélyreható átvizsgálása, ezért az esetleges problémák elkerülése végett nem célszerű adatkérés útján beszerezni. A változékonny adatok mentése során, mivel azok ismételt és azonos tartalmú lementésére nincs lehetőség, ezért az adatmentés lefolytatása kell, hogy garanciális szabályokkal legyen körülbástyázva, amelyek többek között a dokumentáció és a használt eszközökre vonatkozó szabályokat, valamint az eljáró személyre vonatkozó alapvető ismereteket és rendelkezéseket foglalja magába.

A helyszínen történő adatmentés nemcsak fizikai értelemben vett személyi számítógépekről és laptopokról történhet, hanem virtuális eszközökről egyaránt. Ami a virtuális számítógépeket illeti, alapvetően egy meglévő számítástechnikai készüléken futtatható virtualizált rendszerekről beszélünk. Szimulált számítógépek, amelyek egy már rendelkezésre álló számítógépen futnak. Előnye, hogy mivel egy szimulált, virtuális rendszerről beszélünk, ezért amit benne végzünk munkafolyamatokat akár destruktív, megismerési vagy kísérleti jelleggel, nem befolyásolják sehogyan a rendes számítógépünk működését. Napjainkban az Oracle és a VMware szoftvercég virtualizációs szoftverei a legelterjedtebbek, nevezetesen Oracle VM Virtualbox³⁸ és VMware.³⁹ A legfontosabb hardwarebeállítás talán a rendelkezésre bocsátott memória mérete,⁴⁰ amely a tényleges fizikai memóriánkból vesz el. Ez lehet 1-2 GB RAM alatt vagy felett.

³⁸ Oracle VM VirtualBox (<https://www.virtualbox.org/>) Megtekintve: 2021.09.22.

³⁹ VMware Workstation Player (<https://www.vmware.com/products/workstation-player.html>) [2021.09.22]

⁴⁰ Fehér Krisztián: Hackertechnikák: Útmutató valódi hacker módszerek biztonságos kipróbálásához, BBS-INFO kiadó, 2018., 33. oldal

Az egyik legjelentősebb előkészületi fázis a rendőrség által biztosított céladathordozó fizikai felülíráson alapuló teljes törlése,⁴¹ angol szaknyelven „wipe”-olása. Ekkor a külső adathordozót, jellemzően pendrive-ot vagy külső merevlemezt csatlakoztatjuk a rendőrségi számítógéphez, és a célszoftverrel megkezdjük az adathordozó címezhető szektorainak a feltöltését logikai nulla értékekkel, azaz bitről bitre átírjuk a tárhelyét. Erre praktikus a CCleaner⁴² nevű alkalmazást használni, mert pl.: a 64 GB-os méretű pendrive-ot is képes körülbelül másfél óra alatt teljesen lewipeolni, amely egy gyors folyamatnak tekinthető. A folyamat befejezésekor egy teljes egészében üres adathordozót kapunk, amely megfelelő lesz a külső helyszínen történő adatmentésre. Ezt a procedúrát azért célszerű a RAM memória mentése előtt végrehajtani, mert amennyiben korábbi adatokat tartalmaz a külső adathordozó, úgy az ügghöz nem kapcsolódó anyag maradhat rajta. Az adathordozó wipeolásával ez kiküszöbölhető. Ráadásul a későbbiekben is bármikor használhatjuk újra vagy kicserélhetjük a korábban memóriamentésre használt adathordozót, mindössze dokumentálni kell az elektronikus adat áthelyezését, utána pedig bitről bitre törölni kell annak tartalmát.

Számítógépek, laptopok RAM memóriájának vizsgálatánál kulcsfontosságú megemlíteni, hogy elsődlegesen külső helyszínen történő adatmentés során szereshető meg az adathordozó adattartalma, többnyire az eljáró hatóság tagjai által, a vizsgálata viszont labor körülmények között, többnyire igazságügyi informatikai szakértő vagy szaktanácsadó által történik. Egyedül a Windows rendszerek esetében lehetséges korábbi memóriatartalmakat rögzíteni. Ebből adódóan alaposan fel kell készülni az eljárási cselekményre, mert mindössze azok az eszközök állnak rendelkezésre és használhatók, amiket a nyomozók magukkal vittek. Hiánypótlásra esetlegesen van lehetőség, de a kényszerintézkedés időtartama a mulasztásnak köszönhetően elhúzódhat. Az eljárási cselekményt következőképpen úgy kell előkészíteni és lefolytatni, hogy az eljárás ésszerű időn belül befejezhető legyen, az eljárási cselekmény megismétlése vagy újabb eljárási cselekmény elvégzése lehetőleg ne váljon szükségessé.⁴³

A RAM memória rögzítése rövid időn belül befejezhető. Napjainkban erre a célra létrehozott lemez- és memóriakép készítésére alkalmas szoftverek, modulok önállóan futtatható változatával, mint pl.: FTK Imager Portable⁴⁴ egy 8 GB-os memória adattartalma az USB port adatátviteli sebességétől függően néhány perc alatt kivitelezhető. Az FTK Imager ingyenesen

⁴¹ MISZK 6/2020 Módszertani levél 27. oldal

⁴² Ccleaner (<https://www.ccleaner.com/ccleaner/download>) Megtekintve: 2021.09.20.

⁴³ Nyer. 38 § (1) bek.

⁴⁴ FTK Imager Portable (<https://accessdata.com/product-download/ftk-imager-lite-version-3-1-1>) [2021.09.13.]

hozzáférhető a weboldalukon a nyomozó hatóságok számára egy regisztrációt követően. Nemcsak memóriamentést végez, hanem a hash kulcs kiszámítását. Ennek a szoftvernek köszönhetően könnyedén hozhatunk létre hitelesített másolatot a memória adattartalmáról. Fontos megjegyezni, hogy a memória méreténél nagyobb kapacitású adathordozóval rendelkezzen az eljáró hatóság, mert a memóriamentés során létrejövő memóriakép mérete körülbelül 20-30%-kal nagyobb lesz, mint maga a RAM. Ráadásul azért szükséges önállóan futtatható változatot elhelyezni az USB meghajtóra, mert ezek az alkalmazások olyan munkameneteket indítanak el a számítógépen vagy laptopon, amelyhez rendszergazdai jogosultság szükséges. Ideális esetben egy külső helyszínen ez sem jelent problémát, kivéve, ha egy cégnél vagy intézményben történne a memóriamentési folyamat, és a rendszergazdai jóváhagyáshoz jelszót kér a készülék. Abban az esetben, ha 64 vagy akár 128 GB operatív memóriával rendelkezik, a munkafolyamat ugyan elhúzódhat, de végrehajtható. Amennyiben a tervezési szakaszban kiderül, hogy a külső helyszínen összetett számítógépes rendszerekre, hálózatra számíthat a nyomozó hatóság, úgy érdemes szakértőt kirendelni.⁴⁵ Szaktanácsadó igénybevételével érdemes már az eljárási cselekmény megkezdése előtt eljárni, mert különleges szakértelmet igényel a végrehajtás.

A virtuális számítógépek RAM memóriájának vizsgálatánál felmerül a kérdés, hogy egy szimulált számítógépnek miként lehet az adathordozóját vizsgálni, ami fizikailag van benne a használt számítástechnikai eszközökben. A válasz egyszerű, mivel a virtuális számítógépek rendelkeznek egy olyan beépített funkcióval, amely egy úgynevezett pillanatképet⁴⁶ (angol szaknyelven snapshot) rögzít az éppen futó szimulált környezetről, valamint a memóriájának adattartalmáról. Ezzel egy .vmem kiterjesztésű fájl keletkezik, amely többek között a Volatility⁴⁷ nevű alkalmazással is elemezhető. A fizikailag meglévő számítógép vagy laptop esetében pedig amennyiben FTK Imager-t használunk, akkor egy .mem fájlformátum keletkezik a RAM memória mentésekor.

A memória vizsgálata már nem a külső helyszínen történik, mivel egy hosszabb művelet és órákat vehet igénybe a releváns digitális adatok kinyerése. Ilyenkor a forenzikus másolat adattöredékeiből történik az adatok összeállítása (angol szaknyelven file carving) különböző szoftverek segítségével. A folyamat teljesítését követően a digitális bizonyítékok elérhetővé és olvashatóvá válnak az adatösszességéből. A következőkben a már korábban említett bizonyítási

⁴⁵ Be. 189. § (1) bek.

⁴⁶ Memory Forensics for Incident Response (<https://www.varonis.com/blog/memory-forensics/>) [2021.10.06.]

⁴⁷ Volatility Foundation (<https://www.volatilityfoundation.org/>) Megtekintve: 2021.09.22

cselekmények és kényszerintézkedések, mint a szemle, a kutatás és lefoglalás kerülnek részletezésre.

4.1. A szemle

A számítógépek forenzikus vizsgálata megtörténhet a szemle, mint bizonyítási cselekmény keretein belül. Jogi szabályozása az új büntetőeljárási törvényben kerül részletezésre. „Szemlét a bíróság, az ügyészség vagy a nyomozó hatóság rendel el és tart, ha a bizonyítandó tény megismeréséhez vagy megállapításához személy, tárgy vagy helyszín megtekintése, illetve tárgy vagy helyszín megfigyelése szükséges.”⁴⁸ A szemle jogi értelemben egy bizonyítási eljárás, amely alkalmas arra, hogy az esemény szempontjából releváns nyomok, anyagmaradványok, elváltozások jogszerűen, hitelesen hivatkozhatóan felkutatásra és rögzítésre kerüljenek. A kriminalisztikában helyszíni szemleként került meghatározásra ez az eljárásjogi alakíthatósághoz kötött nyomozási cselekmény, amelynek eredménye segíti a felderítést és a bizonyítást, továbbá adatokat, információkat szolgáltat a nyomozáshoz, illetve verziók felállítását segíti, erősíti vagy cáfolja.

A számítógépes rendszernek, beleértve az operatív tárnak az alaposabb vizsgálata szükséges lehet azoknak a digitális nyomoknak az összegyűjtésére és rögzítésére, amelyeket a bűncselekmény elkövetője a bizonyítandó ténnyel kapcsolatban hátrahagyott. A vizsgálat során a szemle szabályait értelemszerűen alkalmazni kell. Amennyiben az információs rendszer, vagy adathordozó átvizsgálása valamely okból különleges szakértelmet igényel, akkor az elektronikus adatok összegyűjtésére szaktanácsadó vagy informatikai szakértő rendelhető ki. A szaktanácsadó kirendelése esetén ugyanazon ügyben később szakértőként már nem rendelhető ki. A bizonyítás szempontjából a jelentős körülményeket részletesen kell rögzíteni a jegyzőkönyvben, mert egy irreverzibilis folyamatról van szó. Szükség esetén kép- vagy hangfelvételt kell készíteni, és a jegyzőkönyvhöz csatolni.

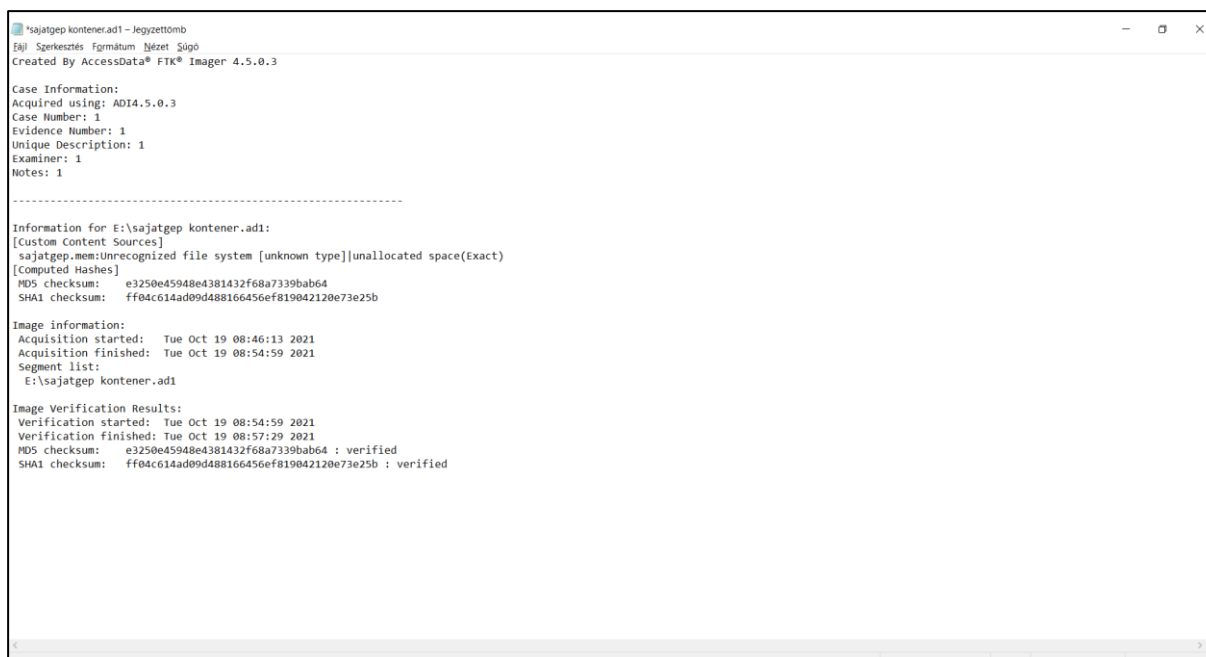
Az adatmentés folyamatáról részletes jegyzőkönyv, jelentés vagy feljegyzés készül, tartalmazva a folyamatokat, megállapításokat, eredményeket. Az adatokról egy image-fájl, azaz képfájl készül. Hitelességének és az adatok integritásának megőrzése érdekében kriptográfiai hasítófüggvények eredményeként létrejövő hasító értékkel,⁴⁹ röviden hash-kulccsal látják el, és

⁴⁸ Be. 207. § (1) bek.

⁴⁹ A Magyar Igazságügyi Szakértői Kamara 6/2020 számú Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről, 2020, 10. o. (https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf) Letöltve: 2021.08.23.

külső adathordozóra, pl.: USB pendrive-ra kerül rögzítésre. Egy matematikai függvény alkalmazásának köszönhetően bármekkora adatösszességet rövid terjedelmű karaktersorrá csökkenthetjük. A kriptográfiában használt gyakori algoritmusok az MD5, SHA1,2,3. Alkalmazási szempontból az SHA1-et a legajánlatosabb használni, mert a létrehozási ideje a legrövidebb. A hash-kulcsot, mint egy digitális ujjlenyomatot kell értelmezni. Minden eltérő adattartalom egyedi hash-kulccsal rendelkezik. Az adattartalom módosulása esetében a teljes ellenőrzőösszeg megváltozik, összehasonlításuk esetén gond nélkül észlelhető a változás, biztosítva ezzel az adatok eredeti állapotának megőrzését. Más eszközre történő másolás, illetve a fájlnev módosításával a hasító érték nem fog megváltozni, mert a név és kiterjesztés fájlrendszerben kezelt adatok. Így a lefoglalt elektronikus adatok a szakértő vagy szaktanácsadó által az eljárás bármely későbbi fázisában feldolgozható marad, illetve eredetisége kizárólag az ellenőrző összeg feljegyzésével a bíróság előtt hitelt érdemlően bizonyítható. Változtatásra kizárólag részletes dokumentáció és jogszabályi, szakmai előírások betartásával nyílik lehetőség.

Egy mintapélda, hogy a jegyzőkönyvben miként kell feltüntetni a RAM memória lefoglalását: A szemle keretein belül a gyanúsított bekapcsolt állapotban lévő számítógépén/laptopján a 8 GB méretű operatív tár teljes tartalmáról történő másolat készítésével egy 9,07 GB méretű memóriakép került lefoglalásra, melyet a memoriakép.ad1 nevű, 4 GB méretű konténerfájlba tömörítettünk. A lefoglalt adatállomány SHA1 hash azonosítója: Ae6427903b65f2e9843b2. Az adatot egy V7 64 GB típusú, XY123456 sorozatszámú pendrive-ra másoltuk. Az egyszerűség kedvéért a jegyzőkönyvhöz lehet csatolni például az FTK jelentését (report), amely tartalmazza a releváns adatokat a mentési folyamatokról.



1. kép: FTK Imager report
Forrás: a szerző

Ennek következtében a helyénvaló dokumentáció tartalmazza a lefoglalás módszerét (amely az adathordozóról történő teljes másolatkészítés), az elektronikus adat integritását megőrző hash-kulcsot, valamint az egyszerűbb belső adminisztráció érdekében a memóriafájl nevét, méretét, hozzávetőleges tartalmát. Ezt követően a bűnjeljegyzék készítése sem fog problémát okozni, hiszen a bűnjel tárgya az elektronikus adat, azaz memóriakép, megjegyzésként pedig azt a külső adathordozót rögzítjük, amelyre a helyszíni adatmentés történt. A kutatás és lefoglalás kényszerintézkedésnél a szemle alfejezet keretein belül leírt módszertan számottevően visszaköszön a dolgozat során.

4.2. A kutatás és lefoglalás

A kutatás szabályai kisebb eltérésekkel azonosak a korábbi büntetőeljárési törvényben szereplő házkutatásával. Az eljáró hatóságok nagy általánosságban alkalmazzák ezt a vagyont érintő kényszerintézkedést. Ennek az eljárási cselekménynek a célja a ház, lakás, kert, egyéb helyiség, bekerített hely, jármű átkutatása, illetve információs rendszer vagy adathordozó átvizsgálása a büntetőeljárás eredményes lefolytatásának érdekében. A kutatás a szemléhez hasonlóan, egy eljárásjogi alakisághoz kötött nyomozási cselekmény, amelynek a szabályai az új Be. törvényben kerülnek részletezésre. Elrendelése határozattal történik, amelyet a nyomozó hatóság bocsát ki, kivételes esetekben a bíróság. Halaszthatatlan eljárási cselekmény esetén

utólagosan történik a határozat meghozatala. Célja, hogy megállapítást nyerjen, van-e a kutatást elszenvedő fél vagy más birtokában bizonyítási eszköz, elkobozható dolog. Az említett kényszerintézkedés a személyes jogokat és szabadságot a legjelentősebben befolyásolja, ennek ellenére gyakran alkalmazzák a nyomozás során a célszerűség és eredményesség biztosítása érdekében, nem együttműködő vagy magas szintű informatikai szakismerettel rendelkező eljárás alá vont személy esetében.

A kutatás kriminalisztikai szempontból személyek, illetve dolgok előkerítése, megtalálása céljából a különböző objektumok átvizsgálására kidolgozott eljárások összefoglaló megnevezése. Amennyiben a bíróság nem rendeli el a kutatást, vagy nem sikerül megszerezni utólag sem az elrendelő határozatot, akkor a nyomozási cselekmény eredménye nem használható fel bizonyítékként. Ahhoz, hogy megfelelően elő legyen készítve és tervszerűen történjen a lefolytatása nagyszámú helyszínek esetében, célszerű egy végrehajtási tervet készíteni. Valójában viszont egy több helyszínes, nagy létszámot igénybe vevő eljárási cselekménynél az érdemi rész, hogy a feladatok, felelőségek meghatározottak és személyhez köthetők legyenek, amelyeket az eligazításokon ki lehet adni. A végrehajtásának módja tervezett időpontban, illetve soron kívül történhet. Krimináltaktikai szempontból hangsúlyos parancsnokot kijelölni, aki az eljárásért felelős, továbbá jegyzőkönyvezőt, csomagoló, hardver-vagy szoftveres átvizsgáló személyt. Az alapos megtervezést követően eredményesebben alkalmazható a lefoglalás és kutatás a büntetőeljárás során, az esetlegesen felmerülő anomáliák pedig könnyebben kiküszöbölhetők. A kutatást az érintett személy jelenlétében szükséges végrehajtani. Ha ilyen személy nincs jelen, akkor az érintett érdekeinek védelmére az ügyben nem érdekelt, nagykorú személy jelenlétében kell a kutatást végrehajtani.⁵⁰

„A kutatást akkor lehet elrendelni, ha megalapozottan feltehető, hogy az

- a) bűncselekmény elkövetőjének elfogására,
- b) bűncselekmény nyomainak felderítésére,
- c) bizonyítási eszköz megtalálására,
- d) elkobozható, illetve vagyoneklobzás alá eső dolog megtalálására vagy
- e) információs rendszer, illetve adathordozó átvizsgálására vezet.”⁵¹

Az új büntetőeljárási törvényben az információs rendszer és adathordozó átvizsgálása miatt is elrendelhető a kutatás, így lehetőség nyílik az elektronikus bizonyítékok felkutatására és

⁵⁰ Be. törvény 305. § (2) bek.

⁵¹ Be. törvény 302. § (2) bek.

rögzítésére kényszerintézkedések keretein belül. A RAM memória mérete napjainkban változó, néhány GB-tól indulva egészen 64 vagy 128 GB-ig terjedhet személyi számítógépek és munkaállomások esetén, viszont egy kutatás során a rögzítése a külső adathordozótól és a csatlakozó sebességétől függően rövid időn belül megvalósítható. A 64 GB és 128 GB-os memóriakapacitás még nem széles körben elterjedt, köszönhetően az árának és a kihasználatlanságának. Amennyiben a vizsgálandó információs rendszer, adathordozó vagy beszerzendő elektronikus adat kigyűjtésének végrehajtásához szükséges speciális szakismerettel rendelkező személy, akkor a kutatás és lefoglalás fogatosításakor szakértő rendelhető ki a szakértői névjegyzékből, de szaktanácsadót, illetve szükség esetén a nyomozó hatóság alkalmazásában álló rendszergazdát is bevonhatunk a kényszerintézkedésbe. Megkezdésekor a kutatást elszenvedő felet, feleket el kell távolítani az adott elektronikai eszköz közeléből, és a fizikai hozzáférését is akadályozni szükséges, nem hagyható magára egészen az eljárási cselekmény befejezéséig. Természetesen célszerű az adott gépre rálátást biztosítani az érintettnek, hiszen így nem tud koholt állításokat megfogalmazni az intézkedéssel kapcsolatban.

Az információs rendszer, vagy jelen esetben adathordozó észlelésére irányuló kutatás során fel kell szólítani a kutatást elszenvedő, vagy általa megbízott személyt, hogy a keresett tárgyi bizonyítási eszköz hollétét fedje fel. A felfedés után is folytatható a kutatás kizárólag abban az esetben, ha feltételezhető, hogy más bizonyítási eszköz pl.: információs rendszer is fellelhető. Az informatikai eszközről indokolt fényképfelvételeket, esetleg videófelvételt készíteni a fellelés környezetéről, a számítógépről és a rajta futó alkalmazásokról, programokról, amelyeknek rögzítése kötelező a jegyzőkönyvben. A bejövő vezeték nélküli kapcsolatot számítógépek esetén az internetkábel leválasztásával, vagy a készülék repülőgép üzemmódba kapcsolással megszakíthatjuk, akárcsak a laptopoknál. Ezzel a folyamattal elkerülhető, hogy egy másik felhasználó, aki kapcsolatban van a vizsgálandó készülékkel távolról egy módosító, vagy destruktív folyamatot indítson el a lefoglalandó eszközön. Abban az esetben, ha egy adatmegsemmisítő művelet zajlik az eszközön, úgy a legcélravezetőbben szükséges az áramellátást megszüntetni asztali számítógépek esetén a tápegységek leválasztásával, laptopok estében az akkumulátor lecsatolásával. Mérlegelni szükséges azonban a hálózatról való leválasztását a vizsgálandó készüléknek, ugyanis a kapcsolat megszakítása esetén megszűnik a hozzáférés a felhőszolgáltatóhoz (cloud computing) és a felhőtárhelyhez, amely eljárási szempontból releváns adatokhoz való hozzáférést hiúsít meg. Ez az úgynevezett „cloud forensic”, azaz felhőalapú vizsgálat.

Napjainkban az adathordozóknak és információs rendszereknek fontos szerepük lehet a bizonyítás során, legyen szó élet elleni, vagyon elleni, gyermekpornográfia bűncselekményről.

A tényállás megismeréséhez és a nyomozás sikeres lefolytatásához kulcsfontosságú szerepe lehet. Ennek értelmében úgy célszerű a kényszerintézkedéseket megtervezni, hogy amennyiben van rá lehetőség, akkor a digitális adatok helyszínen történő adatmentése során rendelkezésre álljon a nyomozó hatóság számára erre a célra kialakított, külső adathordozó és az ehhez szükséges ismeretekkel rendelkező végrehajtó személy.

4.2.1. A lefoglalás

A lefoglalás célja a bizonyítási eszköz, illetve az elkobozható dolog vagy a vagyoneklobzás alá eső vagyon biztosítása a büntetőeljárás eredményes lefolytatása érdekében. A lefoglalás a lefoglalás tárgya feletti tulajdonjogot korlátozza.⁵² Elrendelése a kutatáshoz hasonlóan határozattal történik a nyomozó hatóság, ügyészség vagy bíróság által. Elektronikus adatok lefoglalása esetén akkor alkalmazandó kényszerintézkedés, ha megszerzése egyéb módon nem lehetséges, vagy olyan körülmények állnak fenn pl.: személyi akadály egy nem együttműködő elszenvető fél által, hogy a kényszerintézkedés alkalmazása az eljárás eredményességét biztosítja. Számítógépek, laptopok közvetlen hozzáférésű memóriájának lefoglalása során a RAM által tárolt elektronikus adatok jellemzően nem kerülnek vizsgálat alá, csak rögzítésre és hash-kulccsal hitelesítve, mert erőforrás és időigényes folyamat, így azokat csak beszerezni szükséges a kényszerintézkedés során. Ezt követően labor körülmények között sor kerülhet a korábban rögzített adatok elemzésére az esetek döntő többségében igazságügyi informatikai szakértő által.

Az elektronikus adatok felkutatása, azonosítása után megkezdődhet a lefoglalási folyamat. A gyakorlatban többféleképpen valósulhat meg, amelyet a Be. 315. § (1) bekezdése határoz meg, pl.: másolat készítésével, áthelyezéssel, adathordozó lefoglalásával. A RAM memória esetében csak adatok másolásával valósítható meg a lefoglalási folyamat. Ehhez a nyomozó hatóságnak szüksége van egy üres külső meghajtóra, amely lehet DVD, Pendrive, eSata külső adathordozó. Amikor a számítógép RAM memóriáját mentjük le egy nyomozási cselekmény során, akkor az adathordozó teljes tartalmáról történő másolat készítésével⁵³ valósul meg memóriakép készítésére alkalmas célszoftverrel egy külső adathordozóra. A rögzített adattartalom egy forenzikus másolat lesz. Ebben az esetben egy memóriafájl (angol szaknyelven *memory dump*) lesz a középpontban, és a birtok- vagy tulajdonjog sem kerül korlátozás alá, hiszen nem birtokba vétellel történik a lefoglalás. Mivel a RAM memória adattartalmát, vagyis elektronikus

⁵² Be. törvény 308. § (1) bek.

⁵³ Be. törvény 315. § (1.) bek. c) pont.

adatot foglalunk le másolat készítésével, ezért nem szükséges az elektronikus adatot tartalmazó adathordozót is lefoglalnunk. Ez azt jelenti, hogy nem szükséges szétszerelni a számítógépet vagy laptopot és kivenni belőle annak RAM memóriáját, többek között azért sem, mert ezzel az adattartalma is elveszik.

A memória lefoglalása csak abban az esetben valósítható meg, ha a vizsgálandó készülék bekapcsolt, vagy készenléti állapotban van. Kikapcsolt állapot esetében tilos az eszközt a helyszínen bekapcsolni és memóriamentést végezni. Ennek egyszerű az oka, egy számítógép, illetve laptop esetében minden egyes bekapcsolás során módosulnak az adathordozón lévő releváns adatok. A készenléti, vagy „hibrid alvás” állapot elsősorban azt a látszatot kelti, hogy az elektronikus eszköz ki van kapcsolva. A képernyő sötét és tartalom nélküli, és a LED világítás nem észlelhető. Ellenben egy gombnyomás, vagy egérmozgatás hatására újra aktiválódik, mondhatni „felébred” az alvásból a készülékünk, és üzemkésszé válik. Az alvó üzemmódot a touchpad vagy csatlakoztatott egér mozgatásával, vagy egy funkcióval nem rendelkező gombot megnyomni, pl.: SHIFT, CTRL. Ellenben az ENTER, ESC billentyűk képesek befolyásolni egy háttérben futó alkalmazást, azt elindítani vagy bezárni, ezért kerülendő a használatuk.

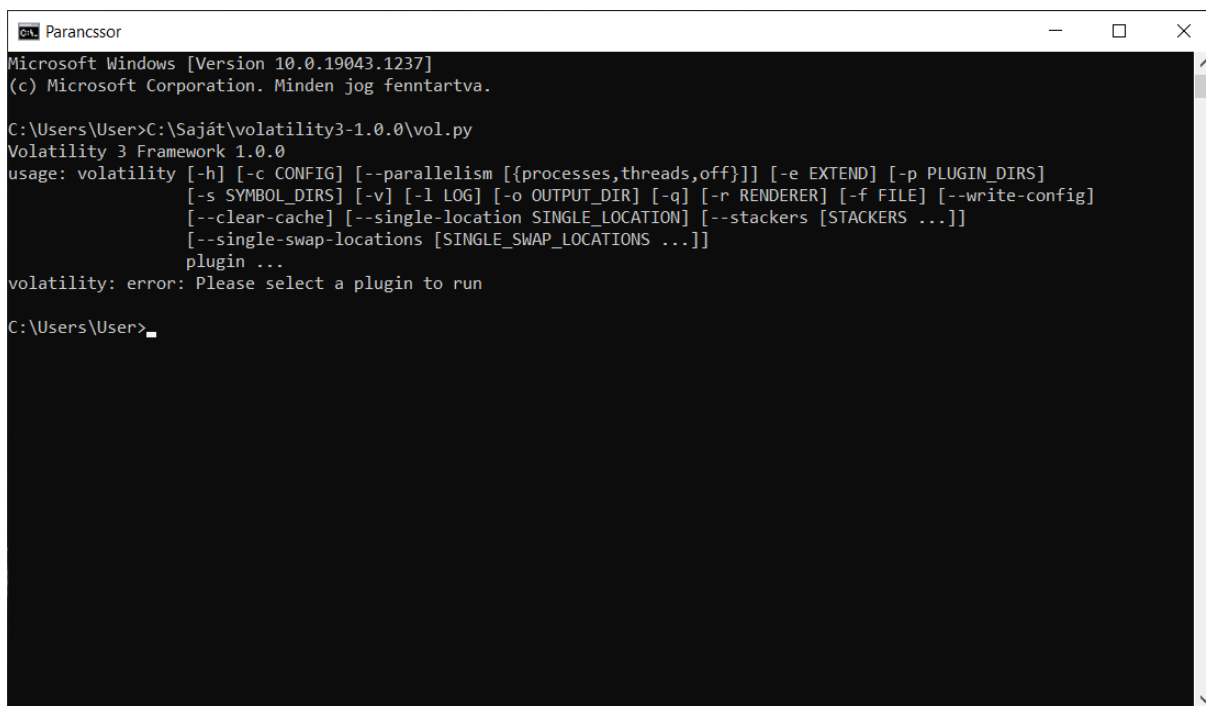
Ami a bekapcsolt, másnéven „élő” rendszereket illeti, ekkor nyílik meg a lehetőség az eljárás vezetőjének elhatározása által külső helyszíni adatmentésre, többek között a RAM memória lementésére. Alapkövetelmény, hogy az intézkedés végrehajtásában részt vevő személyek valamelyike, pl.: szaktanácsadó, rendelkezzen szükséges szakismerettel. Abban a szituációban, ha vállalati környezetben, pl.: egy cégnél található számítógépből vagy laptopból indokolt a helyszíni adatmentés a memóriából, mivel önálló munkaállomásként funkcionálhat az eszköz javasolt a különleges szakértelem miatt igazságügyi informatikai szakértőt vagy szaktanácsadót kirendelni. Otthoni környezetben történő helyszíni adatrögzítés már egyszerűbb eljárásmódot igényel, de a biztonság kedvéért hasonlóan igénybe lehet venni szakértői segítséget.

Mindent egybevetve, az elektronikus adat lefoglalása akár szemle, akár kutatás alkalmával történik, a jegyzőkönyvnek kötelezően tartalmaznia kell néhány ismérvet. Többek között az adatmentés kezdő időpontját, illetve a lefoglalási módszert. Amennyiben másolást hajtottunk végre akkor annak módját, az elvégzett interakciót (fő memória mentése), az alkalmazott szoftvert és verzióját, a rendőrségi adathordozó főbb ismérveit, a tárolt elektronikus adat (memória-fájl) vagy a konténerfájl megnevezését, méretét, kiterjesztését, valamint hash azonosítóját, végül az adatmentés záró időpontját szükséges dokumentálni.

A kényszerintézkedés elvégzését követően, ha más adathordozóra kell áthelyezni a külső helyszínen rögzített memóriefájlt, a bűnügyhöz egy feljegyzés csatolását követően ez szabadon megvalósítható. Ennek eredményeképpen a későbbiekben nem merülhet fel akadály az elektronikus adat más adathordozón tárolása, hiszen a feljegyzéssel a másolás dokumentálva lett, eredetisége pedig a hash-kulccsal leellenőrizhető.

5. OPEN SOURCE ÉS KORLÁTOZOTT ELÉRÉSŰ SZOFTVEREK

A második hipotézisemben azt fogalmaztam meg, miszerint ingyenes, nyílt forráskódú alkalmazások nem képesek olyan mélységben adatokat kinyerni a memóriafájlból, mint a hatóságok részére rendelkezésre álló, kereskedelmi forgalomba kerülő szoftverek. A következő fejezetben megkísérlem alátámasztani, vagy megcáfolni különböző alkalmazások segítségével, fényképfelvételekkel illusztrálva. Elsőként a Volatility⁵⁴ nevű ingyenes, nyílt forráskódú programot fogom górcső alá vetni, amelyet a Volatility Foundation nevű független non-profit szervezet fejleszt. A Volatility egy ránézésre egyszerűen kezelhető, memóriaelemző szoftvernek látszik, hiszen egy parancssori ablakot jelenít meg a program elindulásakor.



```
Parancssor
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\User>C:\Saját\volatility3-1.0.0\vol.py
Volatility 3 Framework 1.0.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                [--clear-cache] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                plugin ...
volatility: error: Please select a plugin to run

C:\Users\User>
```

2. kép: A Volatility kezelőfelülete

Forrás: a szerző

Segítségével hálózati kapcsolatok, háttérfolyamatok és kártékony kódok programjai is olvashatók a rögzített memóriafájlból. Ráadásul 2020 februárjától jelentős fejlesztéseken ment keresztül a program, és megjelent a Volatility3, amely sokkal kezelhetőbbé és teljesítményoptimalizálttá vált a felhasználók számára.

⁵⁴ Volatility Foundation <https://www.volatilityfoundation.org/> Megtekintve: 2021.09.25.

Parancssor

C:\Users\User>C:\Saját\volatility3-1.0.0\vol.py -f C:\Saját\Win10.mem windows.pslist

Volatility 3 Framework 1.0.0

Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0x87355040	162	-	N/A	False	2021-04-02 17:54:30.000000	N/A
88	4	Registry	0x873e58c0	4	-	N/A	False	2021-04-02 17:54:23.000000	N/A
384	4	smss.exe	0x8e892500	2	-	N/A	False	2021-04-02 17:54:30.000000	N/A
516	504	csrss.exe	0x8e60d480	10	-	0	False	2021-04-02 17:54:44.000000	N/A
592	504	wininit.exe	0x936a3040	1	-	0	False	2021-04-02 17:54:46.000000	N/A
600	584	csrss.exe	0x936a60c0	12	-	1	False	2021-04-02 17:54:46.000000	N/A
656	592	services.exe	0x936893c0	10	-	0	False	2021-04-02 17:54:46.000000	N/A
692	584	winlogon.exe	0x9369b040	5	-	1	False	2021-04-02 17:54:47.000000	N/A
744	592	lsass.exe	0x93648040	9	-	0	False	2021-04-02 17:54:48.000000	N/A
844	592	fontdrvhost.ex	0x936e98c0	5	-	0	False	2021-04-02 17:54:49.000000	N/A
840	692	fontdrvhost.exe	0x93695040	5	-	1	False	2021-04-02 17:54:49.000000	N/A
856	656	svchost.exe	0x936a6800	24	-	0	False	2021-04-02 17:54:49.000000	N/A

3. kép: Volatility 3 munkafolyamatok Forrás: a szerző

Ennek ellenére emelt szintű informatikai tudást igényel a gördülékeny használata, ugyanis a használata előtt olyan kötelező szoftvereket kell a készülékünkre letölteni, mint a Python⁵⁵ elnevezésű programozási nyelv, valamint annak elemző modulja, a Pefile.⁵⁶ A megnyitása után a parancssorba is karakterre pontosan kell bevinni az utasításokat annak érdekében, hogy lefuttatható legyen az alkalmazás, ami rendszerint okozhat némi fejtörést. Előnye tehát, hogy bárki számára hozzáférhető és elsajátítása után végtelenszer végrehajtható rajta a memória elemzése Windows, Linux, macOS 32 és 64 bites memóriafájlokból, továbbá virtuális számítógépekből. Hátránya, hogy memóriamentést nem lehet vele végezni, illetve használata informatikában jártasabb felhasználók számára ajánlott.

A Rekall⁵⁷ nevű alkalmazás alapjaiban véve olyan memóriaelemző keretrendszer, mint a Volatility. Alkalmas 32 és 64-bites memóriaképek elemzésére a parancssori segédprogramba bevitt utasításokat követően. A különbség az, hogy 2017 novembere óta érdemben nem fejlesztik, elavultságának köszönhetően inkább régebbi operációs rendszerek memóriájának elemzésére szolgál.

⁵⁵ Python <https://www.python.org/> Megtekintve: 2021.09.25.

⁵⁶ Python PE elemző modul <https://pypi.org/project/pefile/> Megtekintve: 2021.09.25.

⁵⁷ Rekall Forensics <http://www.rekall-forensic.com/home> Megtekintve: 2021.09.26.

A Redline⁵⁸ az előbbiekkal ellentétben már egy grafikus felhasználói felülettel rendelkező, memóriakép rögzítésére és elemzésére alkalmas szoftver. A segítségével metaadatokat, hálózati kapcsolatok, munkafolyamatok, böngészési előzmények gyűjthető be. Egyszerű megjelenésének köszönhetően könnyedén kezelhető, valamint részletes használati útmutatóval rendelkezik.



4. kép: Redline főmenü
Forrás: a szerző

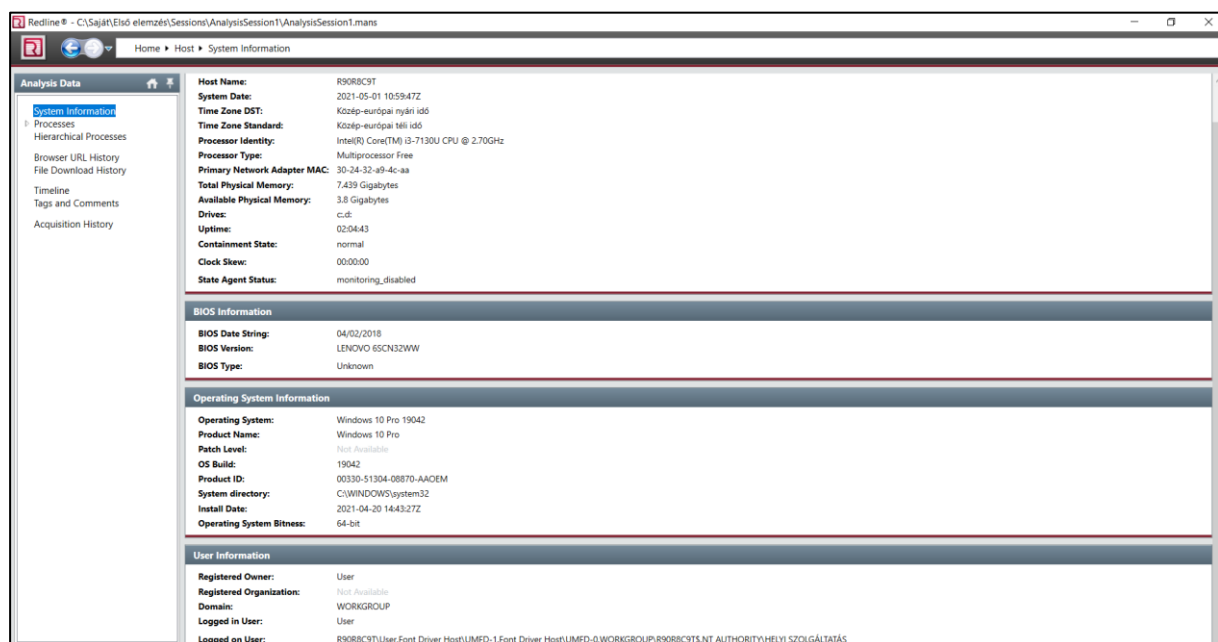
A letöltéséhez szükséges megadni néhány személyes adatot, pl.: teljes név, e-mail cím, munkahely, stb., azonban ezek lehetnek fiktív adatok, mert nem szükséges visszaigazolás az adataink eredetiségéről és bevitelük után automatikusan átirányít egy másik weboldalra, ezzel letölthetővé válik az alkalmazás. Memóriakép mentésekor egy úgynevezett Collector-t fog létrehozni az általunk kiválasztott mappába, amelynek elindításakor megkezdődik a rögzítési folyamat.

⁵⁸ Fireeye Redline <https://www.fireeye.com/services/freeware/redline.html> Letöltve: 2021.09.26.

```
C:\WINDOWS\System32\cmd.exe
Ensuring the proper working directory
".\x64\xagt.exe" -o "C:\Saját\Elemzés\Sessions\AnalysisSession2\Audits" -f "MemoryzeAuditScript.xml"
```

5. kép: Redline munkaablak
Forrás: a szerző

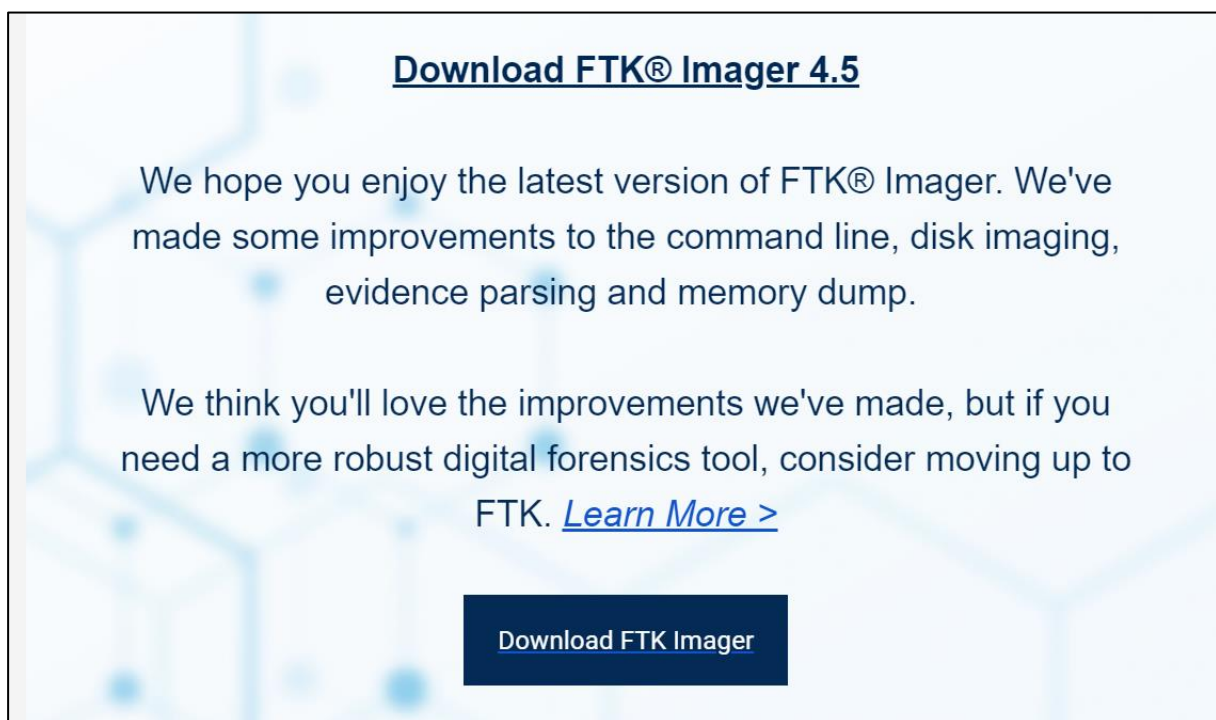
A folyamat végén egy .mans kiterjesztésű memóriefájlt kapunk, amelyet a Redline segítségével elemezhetünk. Az egyszerű grafikus megjelenésnek köszönhetően olyan adatok olvashatóak ki, mint a számítógépünk rendszerinformációi, háttérben futó folyamatok, böngészési előzmények, letöltési előzmények, illetve maga a memóriamegszerzési folyamat.



6. kép: Redline elemzési eredmények
Forrás: a szerző

Előnye, hogy egyszerűen telepíthető és gyakorlás céljából könnyűszerrel kezelhető a letisztult grafikus megjelenésének köszönhetően. Hátránya, hogy kizárólag Windows operációs rendszerek memóriarögzítési és elemzési műveletét támogatja, valamint csak a saját fájlformátumát (.mans) támogatja. Ennek eredményeképpen a korábbi, más szoftverek által lementett memóriafájlok eltérő kiterjesztés miatt a Redline általi memóriaelemzési folyamatokra alkalmatlanok.

Az FTK Imager⁵⁹, mint ahogy már korábban részleteztem, egy forenzikus lemez- és memóriakép készítésére alkalmas szoftver. Egyszerűen kezelhető grafikus felülettel rendelkezik. A Redline-hoz hasonlóan ki kell tölteni a letöltés előtt a személyes adatainkra vonatkozó mezőket. Ami lényeges, hogy az e-mail cím egyezzen meg a valósággal, mert arra kézbesítik a letöltési hivatkozást az adatok bevitelét követően.

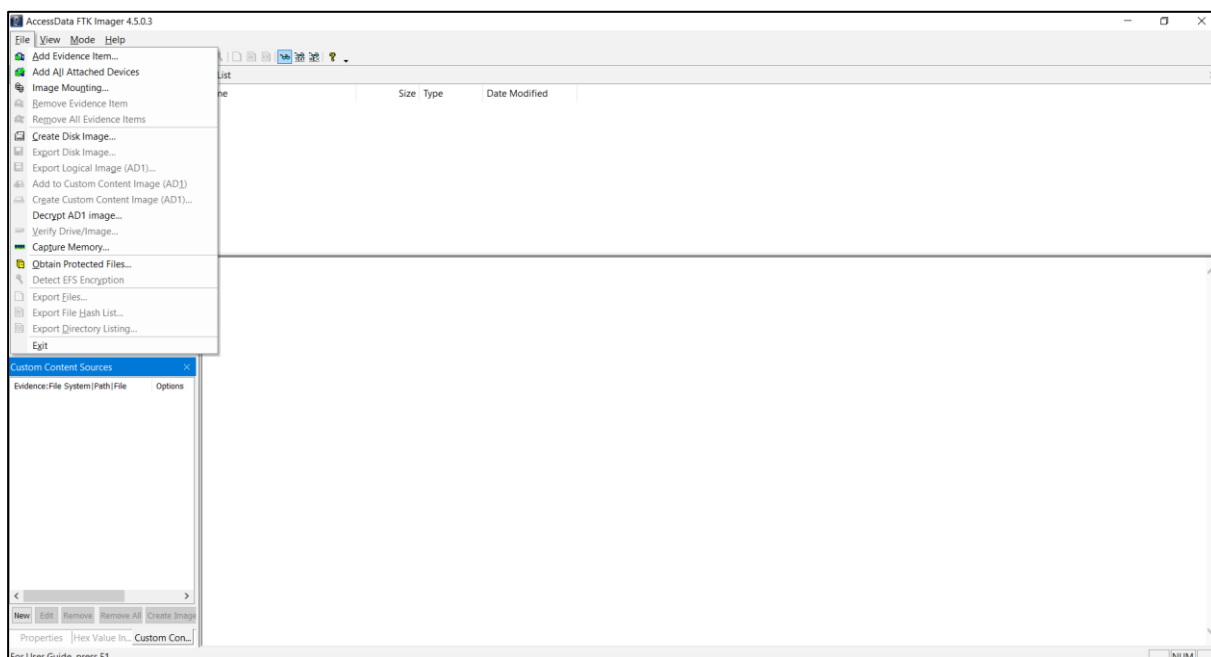


7. kép: FTK Imager letöltése
Forrás: a szerző

A letöltést, illetve telepítést követően már rendelkezésünkre áll egy olyan alkalmazás, amely rövid időn belül hiteles igazságügyi másolatot képes létrehozni. Az FTK Imager képes a memóriarögzítésen (Capture Memory) kívül egy olyan „konténerfájlt” (.AD1) is létrehozni, amely hash-kulccsal van ellátva. Ebből adódóan a memóriakép tömörítésre kerül egy „ad1”

⁵⁹ <https://accessdata.com/product-download/ftk-imager-version-4-2-0> Megtekintve: 2021.09.26.

kiterjesztésű fájlba, illetve egy rövid karakterösszeg lesz a hasító értéke, biztosítva ezzel a rögzített adatok változatlanságának ellenőrzését az eljárás során. A nyomozó hatóságok is előszeretettel alkalmazzák az FTK Imager-t, amennyiben lehetőségük van rá.



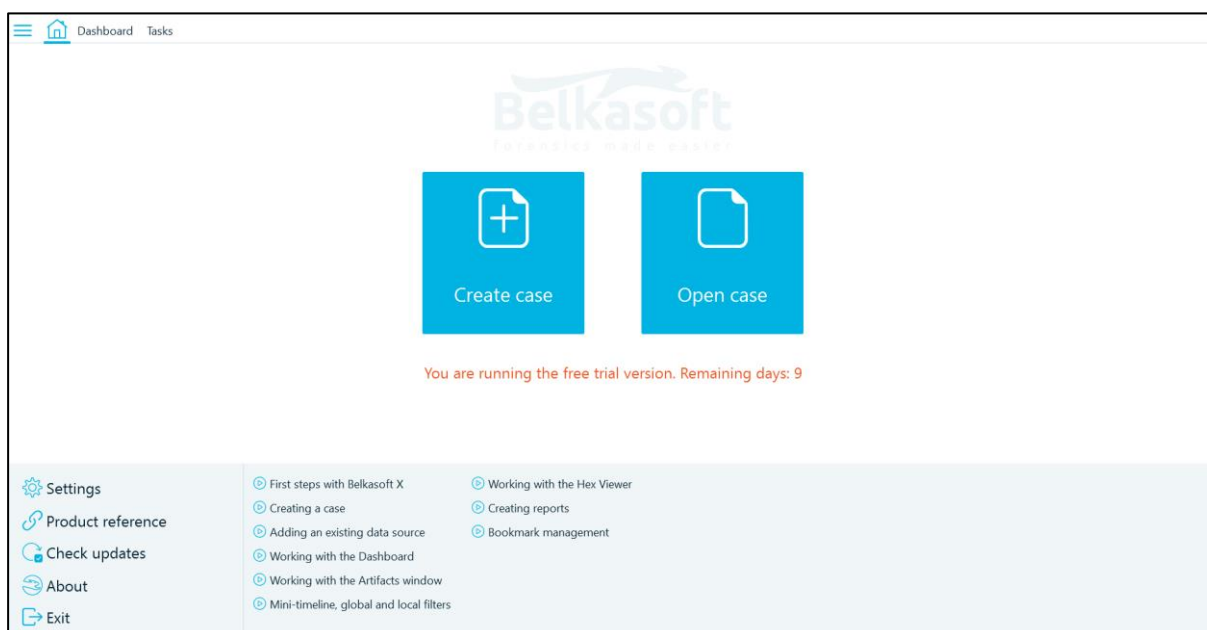
8. kép: FTK Imager főmenü
Forrás: a szerző

Összeségében az FTK Imager egy roppant sokoldalú, szimpla megjelenése miatt valame-lyest egyszerűen alkalmazható szoftver. Előnyei, hogy hiteles forenzikus másolatot készíthe-tünk vele, tömörítési funkciójának köszönhetően biztosítja a rögzített elektronikus adatok in-tegritását, bárki számára elérhető és kipróbálható, ezáltal remek választási lehetőség a gyakor-lásra 32 és 64 bites operációs rendszerek memóriájának rögzítése esetén. Hátránya, hogy me-móriaelemző modullal nem rendelkezik, így ahhoz egy másik számítógépes programot indokolt igénybe venni.

5.1. Zárt forráskódú alkalmazások

Megfigyelhető, hogy jó néhány ingyenes, nyílt forráskódú memóriamentésre és elem-zésre szolgáló szoftver fellelhető az interneten. A következő alkalmazások jelenleg már korlá-tozottabb elérésűek, és túlnyomóan anyagi vonzattal rendelkeznek ahhoz, hogy alkalmazzuk őket.

A Belkasoft Evidence Center X⁶⁰ egy olyan meghatározó terméke a Belkasoft cégnek, amely a számítógépeken, laptopokon, mobiltelefonokon lévő digitális bizonyítékok összegyűjtésére és vizsgálatára szolgál, valamint egyszerű grafikus megjelenési felülettel rendelkezik. Nemcsak a RAM memóriát, hanem a mobiltelefonok adattartalmát és a felhőszolgáltatások igazságügyi elemzését ugyancsak támogatja. Nemzetközi szinten közismert szoftverről van szó, amelyet Európában és az Egyesült Államokban is előszeretettel alkalmaznak a különféle katonai szervezetek, nyomozó hatóságok, igazságügyi informatikai szakértők. Ebből kifolyólag nem meglepő, hogy a programcsomag elérhetősége kizárólag a kereskedelmi forgalomban történő megvásárlása után válik elérhetővé. Ami az igénylését illeti, személyes adatainkat és munkahelyünket, beosztásunkat megadva, az általunk kiválasztott alkalmazás (ami jelen pillanatban Belkasoft Evidence Center X) megjelölését követően néhány munkanapon belül, a megadott e-mail címen keresnek fel minket a cég ügyfélszolgálatáról, amelyben szükség esetén indokolni kell a szándékot a szoftver felhasználására vonatkozóan. Amennyiben pozitív elbírálásra kerül sor, egy letöltési linket kézbesítenek az e-mail címünkre, érvényessége pedig körülbelül 2 hét időtartam. A termék próbaverziója 30 nap, utána elő kell fizetni a későbbi használatához.



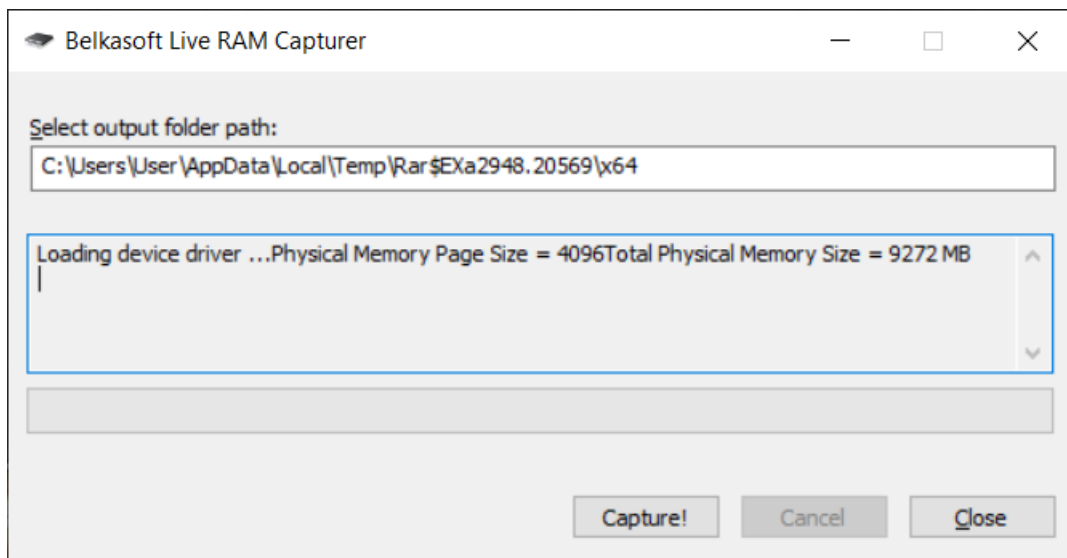
9. kép: Belkasoft Evidence Center X
Forrás: a szerző

Ami viszont kivétel, az a Belkasoft Live RAM Capturer,⁶¹ amelyet az igénylést követően amennyiben letöltjük a készülékünkre, akkor nem meghatározott, hanem korlátlan ideig rendelkezésünkre áll. Mellesleg a RAM Capturerhez nem szükségszerű valós adatokat begépelni,

⁶⁰ Belkasoft Evidence Center X (<https://belkasoft.com/x>) Megtekintve: 2021.09.28.

⁶¹ Belkasoft Live RAM Capturer (<https://belkasoft.com/ram-capturer>) Megtekintve: 2021.09.29.

pusztán elegendő fiktív személyes adatokkal kitölteni a mezőket. Egyedül az e-mail címnek indokolt valódinak lennie, mert arra a levelezési fiókra kézbesítik a letöltési hivatkozást. Kompatibilis minden Windows 32 és 64 bites operációs rendszerrel, valamint külső adathordozóról futtatható adminisztrátori jóváhagyás és előzetes telepítés nélkül.



10. kép: Belkasoft Live RAM Capturer főmenü
Forrás: a szerző

Ami a RAM elemzését illeti, a memóriakép betöltését követően lehetőségünk van kiterjesztett elemzési folyamatot végrehajtani. A memóriaképben lehetőségünk van böngészési előzményeket, rejtett és folyamatban lévő munkafolyamatokat, felhőszolgáltatásokat, közös-

Task	% completed	Status	Time	Elapsed
Analyzing 'C:\Saját\sajatgep.mem'	100%	The operation completed with errors	4/13/2021 8:12:55 AM	2:14:52
Analyzing carved and embedded data	100%	The operation completed with errors	4/13/2021 10:17:45 AM	0:10:03
Carving the data source 'sajatgep.mem'	100%	The operation completed successfully	4/13/2021 9:33:32 AM	0:44:12
Suspicious process name analysis for 'C:\Saját\sajatgep.mem'	100%	The operation completed successfully	4/13/2021 9:33:28 AM	0:00:01
Initializing the data source 'C:\Saját\sajatgep.mem'	100%	The operation completed successfully	4/13/2021 8:12:55 AM	1:20:33
Deleting the data source 'sajatgep.mem'	100%	The operation completed successfully	4/13/2021 8:10:35 AM	0:00:12
Analyzing 'C:\Saját\sajatgep.mem'	100%	The operation completed successfully	4/13/2021 8:09:53 AM	0:00:04

Total: 8 Shown: 8 Checked: 0

Cancel checked

11. kép: Belkasoft Evidence Center X munkafolyamatok
Forrás: a szerző

ségi média fiókokat, elektronikus leveleket, képtörödékeket valamint egyéb állományokat vizsgálat alá venni. Az általunk elindított munkamenetek könnyedén nyomon követhetők a „Tasks” menüpont alatt.

A vizsgálat időtartalma egyenesen arányos annak részletességével. Amennyiben a program által felajánlott opciók közül mindenre szeretnénk kiterjeszteni az elemzési folyamatot, legyen szó pornográfgyanús és kábítószergyánús adattörödéktartalmakról, úgy hosszú órákig, akár napokig is eltarthat a keresési művelet. Cserébe egy részletgazdag eredményt kapunk, amelyben nagy eséllyel megtalálható lesz az általunk keresett elem.

Link	Last visit time (UTC)	Last visit time (local)	First visit time (UTC)	First visit time (local)	Search term
Visited: Felhasználó@https://	2021. 04. 02. 19:13:16				
Visited: Felhasználó@https://	2021. 04. 02. 19:13:15				
Visited: Felhasználó@https://	2021. 04. 02. 19:13:12				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:59				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:33				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:29				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:29				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:23				
Visited: Felhasználó@https://	2021. 04. 02. 19:10:23				
Visited: Felhasználó@https://	2021. 04. 02. 19:09:39				
Visited: Felhasználó@https://	2021. 04. 02. 19:09:39				
Visited: Felhasználó@https://	2021. 04. 02. 19:09:29				facebook
Visited: Felhasználó@https://	2021. 04. 02. 19:09:29				facebook
Visited: Felhasználó@https://	2021. 04. 02. 19:09:08				facebook
Visited: Felhasználó@https://	2021. 04. 02. 19:09:08				facebook
Visited: Felhasználó@https://	2021. 04. 02. 19:08:38				
Visited: Felhasználó@https://	2021. 04. 02. 19:08:37				
Visited: Felhasználó@https://	2021. 04. 02. 19:08:37				
Visited: Felhasználó@https://	2021. 04. 02. 19:08:26				

12. kép: Belkasoft Evidence Center X keresési eredmények
Forrás: a szerző

A Belkasoft rendelkezik egy olyan egyedi kiadással, nevezetesen Belkasoft R,⁶² amelynek segítségével nem kell a helyszínen tartózkodni, hanem távoli vezérléssel (remote control) végre lehet hajtani a digitális bizonyítékok begyűjtését és rögzítését, így a RAM memória adat-tartalmát is. Ez hálózati kapcsolat létesítése során valósítható meg, mert egy úgynevezett kém-programot telepítünk a végponti készülékre, az IP cím és port számának megadásával.

Összegezve, a Belkasoft Evidence Center X egy felhasználóbarát, egyszerre több átfogó vizsgálat lefuttatására képes alkalmazás, amelyet hosszú évek óta folyamatosan fejlesztenek a naprakészség érdekében. Ennek köszönhetően nőtte ki magát már egy komplex programcsomaggyá a Belkasoft, magába foglalva számos modult. A gördülékeny használata érdekében ön-álló Youtube csatornáikkal és oktatói videófelvételekkel rendelkezik, ezzel is támogatva az előfizetőket. Mindemellett nemcsak Windows, hanem Mac operációs rendszerrel rendelkezők is alkalmazhatják a Boot Camp⁶³ megnevezésű asszisztens futtatásával.

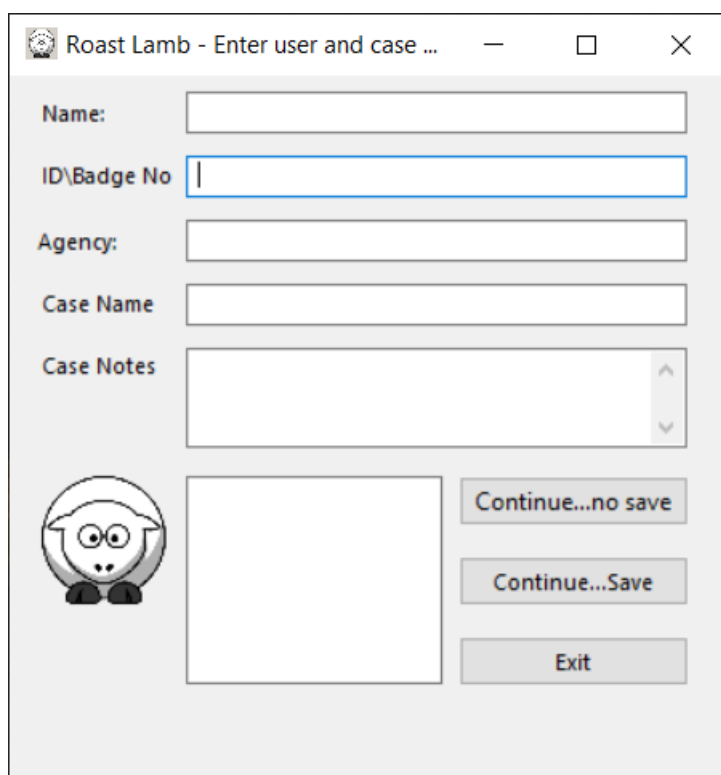
Hátránya, hogy zárt forráskódú. Amennyiben jogosultságot szerzünk használatára, pusztán egy 30 napos időtartamú ingyenes verzió válik elérhetővé, később pedig kötelezően elő kell fizetni a szolgáltatás igénybevételéhez. Kivétel ez alól a korábban említett Belkasoft RAM Capturer, amelyet egyszer letöltve a készülékünkre korlátlanul elérhetővé válik.

⁶² Belkasoft Remote Acquisition (<https://belkasoft.com/r>) Megtekintve: 2021.09.30.

⁶³ Boot Camp segédprogram (<https://support.apple.com/hu-hu/boot-camp>) Megtekintve: 2021.10.02.

Végül, de nem utolsósorban a Roast Lamb elnevezésű memóriaképelemző alkalmazással fogunk megismerkedni. A Roast Lamb a FREETOOL – Free Reliable Tools for Investigating Cybercrime⁶⁴ európai unió által finanszírozott projekt keretein belül került megalkotásra. A program célja a rendvédelmi szervek számára személyre szabott eszközök, szoftverek létrehozása a kiberbűncselekmények elleni fellépéshez, illetve azok nyomozásához.

A Roast Lamb egy grafikus felülettel rendelkező, többplatformos, RAM által tárolt digitális adatok elemzésére alkalmas szoftver. Ez a program több európai nyomozó hatóság, egyetem, és szervezetek együttműködésével jött létre. A korábbiakkal ellentétben már nemcsak Windows 32 és 64 bites, hanem MAC és Linux operációs rendszerek mentett memóriájának elemzésére képes. Platformra lebontva mindegyik verzió rendelkezik egy MD5 hash értékű fájlal, amely a szoftver integritását igazolja.

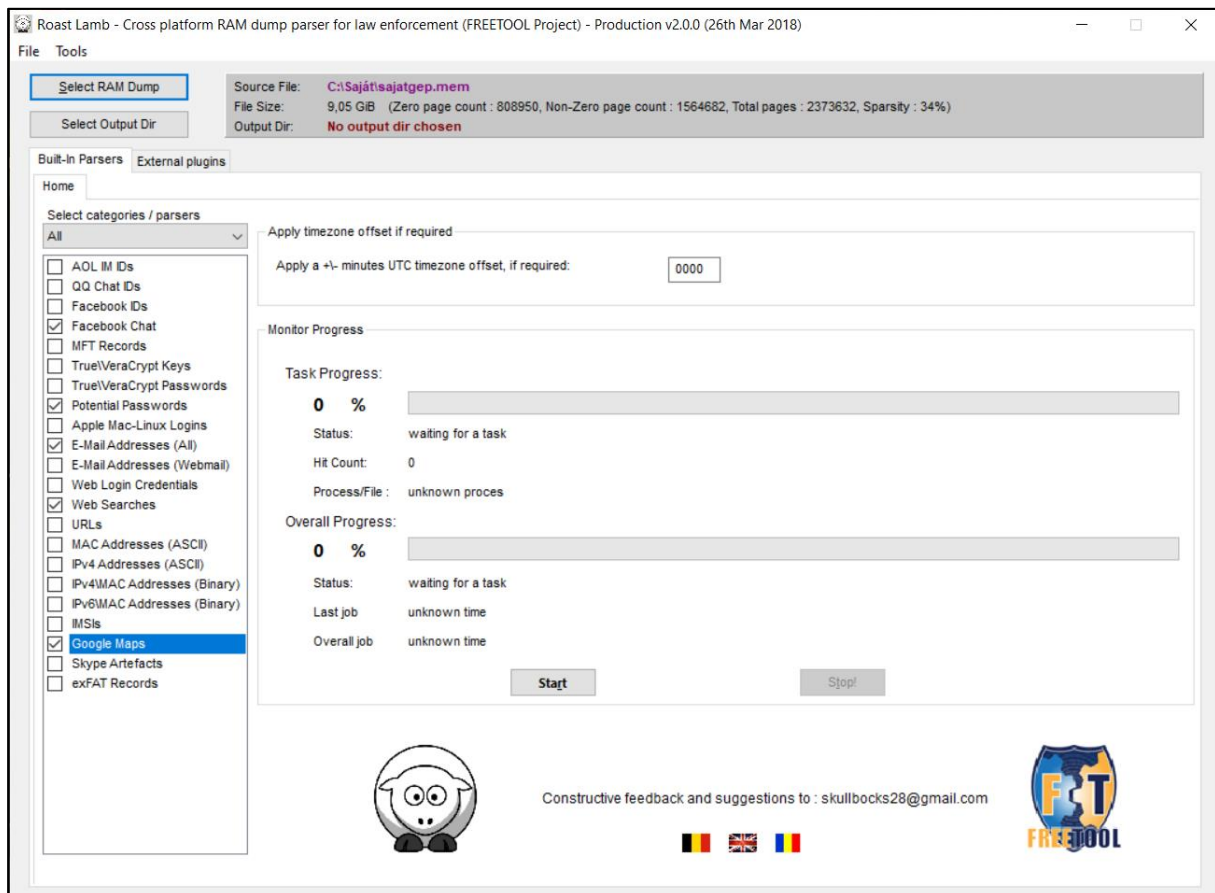


13. kép: Roast Lamb
Forrás: a szerző

Az egyszerű grafikus megjelenésének köszönhetően nem okoz komolyabb fejtörést a program kezelése, emellett rendelkezik egy rövidített, illetve bővített használati útmutatóval is. A megnyitás és mezők tetszőleges kitöltését követően átirányít a Roast Lamb a főmenüre, ahol

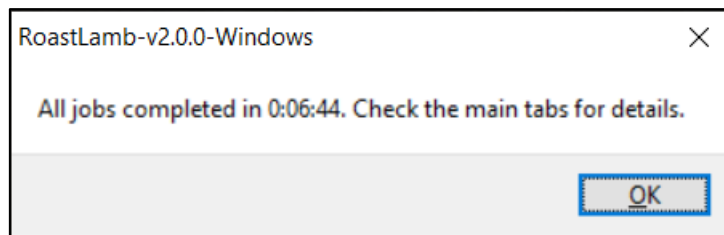
⁶⁴ FREETOOL – Free Reliable Tools for Investigating Cybercrime (<https://thefreetoolproject.eu/>) Megtekintve: 2021.10.04.

a korábban rögzített memóriakép és a kimeneti eredmények mappa kiválasztását követően személyre szabottan tudunk vizsgálati folyamatokat indítani, akár kategóriákra lebontva, mint pl.: lehetséges jelszavak, IPv4 címek, e-mail fiókok, böngészési előzmények, stb.



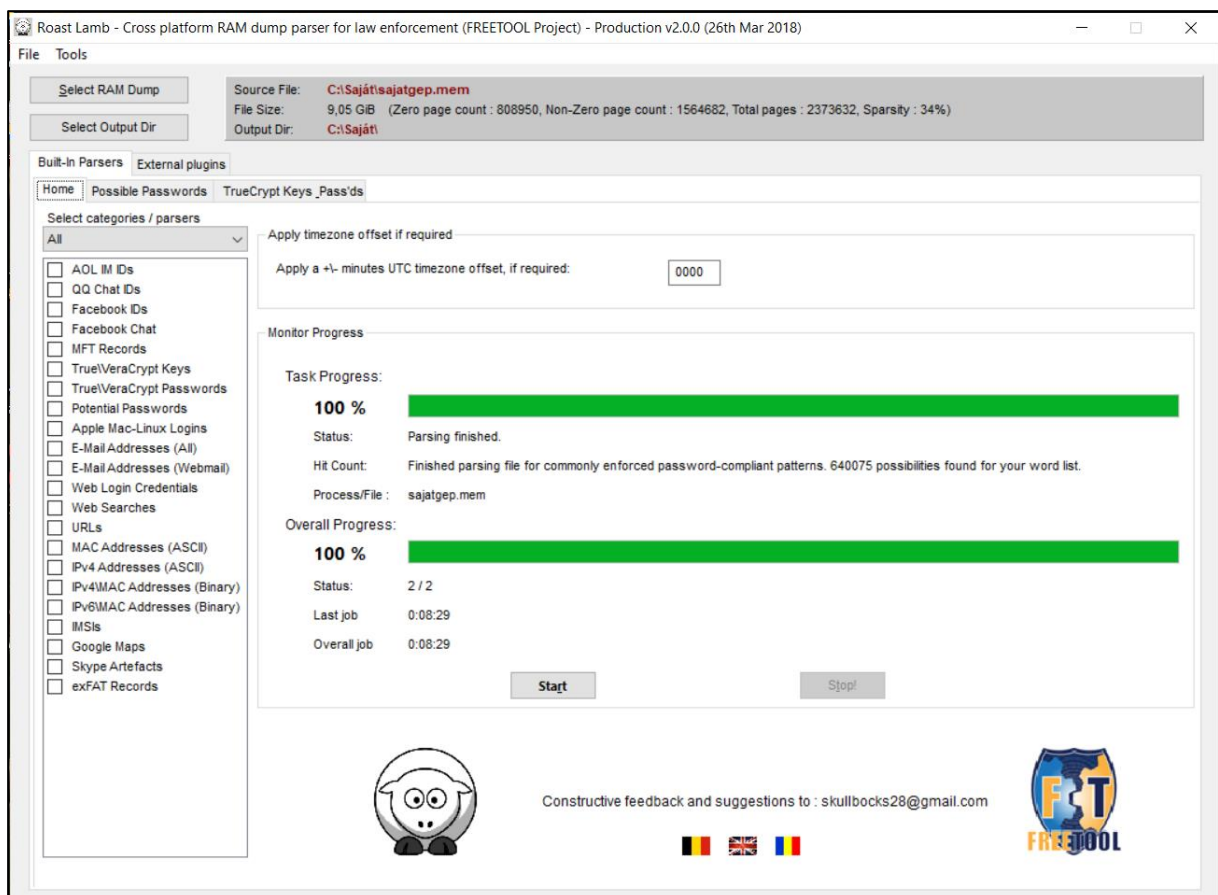
14. kép: Roast Lamb főmenü
Forrás: a szerző

Az keresési opciók bejelölése során megkezdődik a vizsgálati szakasz. Időtartama függ a kiválasztott kategóriák számától, a RAM méretétől és a számítógép/laptop teljesítményétől. Ennek eredményeképpen néhány perctől egészen hosszú órákig, akár néhány napig is megnőhet az elemzési folyamat. Természetesen mérlegelni kell, mely információk lehetnek relevánsak az adott ügyben, és azokra kiélezve néhány kritériumra leszűkítve végrehajtani az eljárási procedúrát.



15. kép: Roast Lamb munkafolyamat
Forrás: a szerző

A művelet befejezésekor két helyen tudjuk megtekinteni a keresett találatokat.



16. kép: Roast Lamb befejezett vizsgálat
Forrás: a szerző

A Roast Lamb-en belül a „Home” fül mellett lefuttatott keresések jelennek meg különálló füleken, vagy az általunk kiválasztott kimeneti könyvtárba kerülnek .xls fájlkiterjesztésben. Egy „OutputHashes” megnevezésű szöveges dokumentumban egyedi MD5 és SHA-1 hash azonosítóval vannak ellátva az befejezett vizsgálati folyamatok, biztosítva ezzel a kimeneti eredmények integritását és a folyamat jogszerűségét.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1		Process	Mail Address	Contextual Result	Hex Offset	Dec Offset																	
2	1	Win10.mem.vmlister	@e1.ru.zipfron	tend.exes&space.comuploadgetinfo&api_key=	svsaleristar@e1.ru.vb	(JlXyVwVa>E\$SCOPhc\wdoHsy,002225B4,2237876																	
3	2	Win10.mem.vwww	.example.com	www.example.com,	cation=	@ leaseRequired@metainfoType@localLicense"	@www.example.com@www.example.com@_PrimaryTileUserID",00234674,2311796																
4	3	Win10.mem.plugin	@videofiledownload.com	illaVFirefoX\Profiles\?????.default\extensions\plugin@videofiledownload.com\I\$mall.TNIOfficia.VT~a,00740898,7604376																			
5	4	Win10.mem.bignetdaddy	.comdownload	trueads.register@havingfunonline.com,earchTerms<key=HomePage</key>download.dynamet.combignetdaddy.comdownload.trueads.register@havingfun,007409C6,7604678																			
6	5	Win10.mem.app	@appenvaena.com	br,5BK*Lastspirevelalalum.comiponitasWlheckipake5Lapp@appenvaena.com.br/img/linagr.eoLl.php/fejcaler/,00850859,8718425																			
7	6	Win10.mr	serviceur=	%8100%pdH"***009B50E,10178799																			
8	7	Win10.mr	serviceur=	%8100%pdH"sofP,009B51A1,10178977																			
9	8	Win10.mem.talosadam13	@gmail.com	,XyvfelhasznIDESKTOP-3FUF68QHMicrosoftAccount:user-talosadam13@gmail.com,%8100%pdH"0**0 P& F16 ",7",009B5253,10179155																			
10	9	Win10.mem.talosadam13	@gmail.com	,XyvfelhasznIDESKTOP-3FUF68QHMicrosoftAccount:user-talosadam13@gmail.com,%8100%pdH"0**PX F516 X ",009B52F4,10179316																			
11	10	Win10.mr	serviceur=	%8100%pdH"***009B539A,10179482																			
12	11	Win10.mr	serviceur=	%8100%pdH"-WinP,009B544E,10179662																			
13	12	Win10.mem.talosadam13	@gmail.com	,XyvfelhasznIDESKTOP-3FUF68QHMicrosoftAccount:user-talosadam13@gmail.com,%8100%pdH"0**0Ea P& F16 Ea ",009B5504,10179844																			
14	13	Win10.mem.nightin	@xaa.pl	,WbJdL5nmljZG@XaAJaClient&check""jassword=&logininightib@xaa.plNMAREKMoje dokumy Kradzare@9E*",00030856,13830998																			
15	14	Win10.mem.talosadam13	@gmail.com	,&csz w D&WClient w"vww"Zl w4P4vaS'8002E0CDA02772@'Hi'talosadam13@gmail.com@b'l'0001133883@'MioftAccou@",00092FAF,14233519																			
16	15	Win10.mem.njq8	@gmail.com	,e.My.ResourcesBrute Force vCoded By: njq8 Email: njq8@gmail.compop3.live.com Sohanad.IABlacle.HMa)",000C2AB9,14428857																			
17	16	Win10.mem.w7	@client.wns.windows.com	,TTop5ku@4Tw.P 7@4Tw -Pz@1 zyD@6WxG~--Pp 8@JP@47@client.wns.windows.com@4Tw.P@8 P@Z9 @Categor",012C0E0A,19664394																			
18	17	Win10.mem.m8	@m8oe@microsoft.com	,ar=1&pctype=wangbarpc&BHO_k+ik3lBancos.SB<a4KxmXx#m8oe@microsoft.com8882ad5e90b4afb6699842fb459f7",01391C4F,20520015																			
19	18	Win10.mem.ownloadetd	@a122.dscg3.akamai.net	,@H_8h=Gp@',) s @4XoXo8l@ mp@ Fh s@WU Client Downloadetd@a122.dscg3.akamai.net0@HHHDownloadMode3",013822EB,20652779																			
20	19	Win10.mem.uninstall	@secureize.biz	,uninstall please send an email at this address: uninstall@secureize.biz YD JG*QK"BSOFTWARE\Micros",01613818,23149336																			
21	20	Win10.mem.wdcp	@microsoft.com	,I\Microsoft\fluency\lmhu-HU\config_tmp.hURIU@+**c@wdcp.microsoft.com.Rhttp://canonicalizer.ucsur,01631DB8,23272888																			
22	21	Win10.mem.support	@eurekalog.com	,ealert level:windows\currentversion\run\default""support@eurekalog.comEa6jBd""2a6bju@createtoolhelp",01760EA4,24514212																			
23	22	Win10.mem.p	@bing.com	, c CooYe @>1 #6@QH66jXw@*Jo(P3 7uhDMruhHrA<x%p@bing.com @_le(k y? C (u9yX Jv=JkplRPC%35y>X O",017F0EB8,25104056																			
24	23	Win10.mem.tsfe	.tra@fichshaping.dsp.microsoft.com	,%OM 7r ml-com+MRz& z 7.n Y@'6nw"vUxMKH 18https://tsfe.tra@fichshaping.dsp.microsoft.comVq WYCanon",01803194,25178516																			
25	24	Win10.mem.d181238	@tuta.io	,hate11 ob Release hate11.pdbcontact by e-mail: d181238@tuta.io or d181238@india.com http://5.1",018E4680,26101424																			
26	25	Win10.mem.d181238	@india.com	,hate11.pdbcontact by e-mail: d181238@tuta.io or d181238@india.com http://5.1.83.182:8000/cg-bin",018E46C5,26101445																			
27	26	Win10.mem.8332	@uminers.bit@mail.ru	,er.Olbat NV000H4*/KO.exe""ohhttp://pool.50btc.com:8332-uminers.bit@mail.ru_tf-pass- 2 Nefyn.A<x""",0197178E,26679182																			
28	27	Win10.mem.vml	@hotmail.com	,@Xsoftware\borland\delphis\antw@sbancos.santander.lreal@hotmail.com RnrectLAIAsnerTrojan:HTML Blaco",01AR1C52,27991127																			

17. kép: Roast lamb vizsgálati eredmények Excel-ben

Forrás: a szerző

Az Excel fájlformátumban jól észrevehető a sorok összemosódása, ezért az átláthatóság érdekében a Roast Lamb-en belül érdemes a lefuttatott kereséseket elemezni. Fontos megjegyezni, hogy az alkalmazás bezárását követően nem lesz lehetőségünk újból azon a felületen megtekinteni a vizsgálati eredményeket, csak az Excel dokumentumban, kivéve, ha újra lefuttatjuk a keresési műveletet. Az „External plugins” menüpontra kattintva a Volatility-t, mint külső kiegészítő szoftvert adhatjuk hozzá a Roast Lamb-hez. Ebből kifolyólag a hálózati kapcsolatok, a rejtett munkafolyamatokat, a kártékony kódokat is elemezhetjük.

Ami tehát a Roast Lamb memóriaelemző szoftvert illeti, előnye, hogy multiplatformos, ezáltal Linux 32 és 64-es disztribúción, Windows 32 és 64 biten, illetve macOS operációs rendszeren is egyaránt lefutatható. Minimalista grafikus és strukturális megjelenésének köszönhetően egyszerűen kezelhető, felhasználóbarát felülettel rendelkezik, amelyben személyre szabottan tudjuk lefuttatni a kutatási folyamatokat, és automatikusan egyedi hasító értékkel látja el a vizsgálatokat, biztosítva ezzel a hitelességet. A Volatility funkciója pedig olyan vizsgálatot eredményez, mintha egyszerre két különböző programmal elemeznénk a memóriaképet.

Hátránya, hogy hosszú órákig, akár napokig is elhúzódhat a művelet, hiba felmerülése és az abból fakadó programleállás következtében kénytelen a felhasználó ismételt lefuttatni az analízist, ami többlet időt igényel. Mellesleg a kimeneti eredményeket az Excel dokumentum összezsúfoltan tartalmazza. Ebből kifolyólag körülményessé válik a keresési folyamat még a beépített kereső algoritmussal is, amennyiben több százezer sort tartalmaz az állomány.

Az eddig megismert alkalmazások döntő többségében Windows 32 és 64 bites operációs rendszerekre lettek programozva. Ez érthető, hiszen napjainkban a Windows számít a legnépszerűbb programrendszernek és dominál a különböző számítástechnikai eszközökön. Ennek ellenére

közismertek a Linux és macOS készülékek, amelyek közvetlen hozzáférésű memóriájának forenzikus vizsgálata másféle megközelítést igényel.

A Linux 32 és 64 bites memóriájának megszerzése a LiME és Microsoft AVML modulokkal valósítható meg. A LiME⁶⁵ (Linux Memory Extractor) egy betölthető kernelmodul (LKM) amely Linux és Linux alapú elektronikus eszközök RAM memóriájának rögzítésére szolgál, és hash kulccsal látja el a memóriaképet. A LiME lehetővé teszi a teljes memóriatartalom rögzítését Android eszközökön⁶⁶ egyaránt. A memóriamentés végrehajtásához tisztában kell lenni az operációs rendszer disztribúciójával vagy kernelszámával. Ezt küszöböli ki a Microsoft AVML⁶⁷ (Acquire Volatile Memory for Linux) memóriarögzítő alkalmazás, amelynél nem szükséges előzetes információk birtokában lennünk ahhoz, hogy a folyamatot sikeresen végre tudjuk hajtani. Mindkét modul parancssori megjelenésű, grafikus felülettel nem rendelkezik, valamint alkalmas 32 és 64 bites operációs rendszerek operatív tárárt rögzíteni. Ezt követően lehetőségünk nyílik a RAM adattartalmának vizsgálatára, amelyet a korábban említett Volatility és Roast Lamb szoftverrel szintén elvégezhetjük.

Végül, de nem utolsósorban, ami a macOS operációs rendszerek közvetlen hozzáférésű memóriájának rögzítését és elemzését illeti, a Mac Memory Reader⁶⁸ (MMR) volt az első eszköz a fő memória Mac rendszerekből történő megszerzésére.⁶⁹ A parancssori segédprogram támogatja a 32 és 64 bites architektúrából történő memóriamentést, valamint ellenőrző összeget kalkulál többek között MD5 és SHA-1 formátumban. Hasonló alkalmazások a Mandiant's Memoryze⁷⁰ és az OSXPmem⁷¹ annyi különbséggel, hogy az OSXPmem a 32 bites verziókat már nem támogatja, illetve a Mandiant's Memoryze memóriaelemzési folyamatok is képes lefuttatni. Az említett szoftverek által mentésre került memóriakép vizsgálatára szintén a Roast

⁶⁵ Linux Memory Extractor – LiME (<https://github.com/504ensicsLabs/LiME>) Megtekintve: 2021.10.05.

⁶⁶ Rushita Dave, Nilay R. Mistry, M. S. Dahiya: Volatile Memory Based Forensic Artifacts & Analysis, Gujarat Forensic Sciences University, 2014, 3. o. (<https://cyberforensicator.com/wp-content/uploads/2018/02/file-serve.pdf>) Letöltés ideje: 2021.10.06.

⁶⁷ Microsoft AVML - Acquire Volatile Memory for Linux (<https://github.com/microsoft/avml>) [2021.10.05.]

⁶⁸ Mac Memory Reader – MMR (<https://www.sans.org/blog/mac-os-forensics-how-to-simple-ram-acquisition-and-analysis-with-mac-memory-reader-part-1/>) Megtekintve: 2021.10.05.

⁶⁹ Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons, Inc., Indianapolis, Indiana, 2014, 781. o. ([https://repo.zenk-security.com/Forensic/The%20Art%20of%20Memory%20Forensics%20-%20Detecting%20Malware%20and%20Threats%20in%20Windows,%20Linux,%20and%20Mac%20Memory%20\(2014\).pdf](https://repo.zenk-security.com/Forensic/The%20Art%20of%20Memory%20Forensics%20-%20Detecting%20Malware%20and%20Threats%20in%20Windows,%20Linux,%20and%20Mac%20Memory%20(2014).pdf)). Letöltve: 2021.10.05.

⁷⁰ Mandiant's Memoryze (macOS) (<https://fireeye.market/apps/211372>) Megtekintve: 2021.10.05.

⁷¹ OSXPmem – Mac OS X Physical Memory Acquisition tool (<https://code.google.com/archive/p/pmem/wiki/OSXPmem.wiki>) Megtekintve: 2021.10.05.

Lamb és a Volatility, valamint az említett Mandiant's Memoryze memóriaelemző alkalmazás vehető igénybe.

6. ESETTANULMÁNY: BITLOCKER⁷²

Egy 2020. decemberi bűnügyben a Büntető Törvénykönyvről szóló 2012. évi C. törvény 204. § (1) bekezdés a) pont-jába ütköző és az (1) bekezdés a) pontja szerint minősülő tizennyolcadik életévét be nem töltött személyről, személyekről pornográf felvétel megszerzésével vagy tartásával elkövetett gyermekpornográfia büntettének megalapozott gyanúja miatt indult ügyben az eljáró hatóság informatikai eszközöket foglalt le, amely vizsgálata szükséges az ügy szempontjából lényeges tények megállapítására.

A határozatában rögzített adatok vizsgálatára és a feltett kérdések megválaszolására a Nemzeti Szakértői és Kutató Központot rendelte ki igazságügyi szakértői vélemény előterjesztésére. A szakértő feladata a nyomozás során lefoglalt eszközök vizsgálata, a kirendelő határozatban szereplő kérdések megválaszolása.

A szakmai ténymegállapítások során egy Lenovo Thinkpad gyártású számítógép vizsgálatára került sor. A vizsgált számítógép egyetlen merevlemezt tartalmazott, amely a gyártói teszt eredménye alapján hibamentesnek bizonyult. Az adathordozón található fájlrendszert tartalmazó logikai egységből (partícióból) 4 db található: P1, P2, P3, P4.

A P1, P2, P4 partíciók az operációs rendszer helyreállításához szükséges állományokat tartalmazzák, méretük összességében alig haladja meg az 5 GB-ot. Ellenben a P3 partíció, amelynek mérete 471 GB, Bitlocker titkosítással védett. A Bitlocker egy olyan adattároló titkosító szolgáltatás, amely segít megvédeni a merevlemezen tárolt adatainkat, így csak azon személyek számára érhetők el, akik jogosultak rá. Feloldásához szükséges helyreállító kulcs (angolul recovery key) a vizsgálat során nem állt rendelkezésre. A számítógép bekapcsolásra került, a kirendelő által biztosított felhasználói adatok segítségével az operációs rendszerben létrehozott felhasználói fiók betöltésre került. A működő operációs rendszer által használt memóriáról (RAM) memóriakép készült, amely alapján a Passware Kit Forensic⁷³ eszköz segítségével a titkosításhoz használt helyreállító adatok kiolvashatók voltak. A kiolvasott helyreállító kulcs segítségével a partíción tárolt adatok vizsgálhatóak voltak.

Az ügygel kapcsolatba hozható felhasználói állományok a P3\Users\gabor mappán belül voltak fellelhetők. A felhasználói állományok egy része munkavégzéssel kapcsolatos, üzleti titkot képezhettek. A „Downloads” mappában egy darab szexuális tartalmú kép volt fellelhető.

⁷² A teljes esettanulmány a Mellékletek fejezetben olvasható.

⁷³ Passware Kit Forensic (<https://www.passware.com/kit-forensic/>) Megtekintve: 2021.10.30.

A képet készítő eszközről, a kép készítésének körülményeiről nem áll rendelkezésre információ. A számítógépen javarészt munkavégzéshez szükséges szoftverek voltak fellelhetők.

Mindent egybevetve, az igazságügyi informatikai szakértői véleményben kiolvasható, hogy a titkosított meghajtó feloldásához elengedhetetlen volt a RAM memória adattartalmának rögzítése. A kártékony kódok felderítése mellett Bitlocker-rel védett partíciók feloldásához a memóriaképből kiolvasható a helyreállító kulcs, amennyiben első körben nem áll rendelkezésünkre. A feloldott logikai egységből további releváns digitális adatok fellelhetősége biztosított.

7. A JÖVŐ, LEHETSÉGES KIHÍVÁSOK

Ami a számítógépek memóriájának vizsgálatát illeti a jövőre nézve, egyértelműnek látszik a memória méretének az exponenciális növekedése. Amíg korábban elegendő volt néhány GB RAM kapacitással üzemeltetni egy személyi számítógépet, úgy napjainkban az átlag felhasználónál is 16 GB memóriára növekedhet. Kivételes esetekben 32, 64, 128 GB-ra, vagy annál többre emelkedhet az operatív tár mérete, felhasználásától függően. Ennek több indoka van, gondoljunk csak a „gamer” számítógépekre, ahol elengedhetetlen a legkorszerűbb számítógép alkotóelemek és tárhelyek megléte, de előfordulhat ez az eset olyan cégeknél és szervezeteknél, ahol nagy teljesítményű számítástechnikai berendezésekre van szükség pl.: NASA. Minél nagyobb egy tárhely, annál több fájl, elektronikus adatot tartalmazhat, ezáltal a lefoglalásuk, elemzésük, feldolgozásuk is időigényesebb folyamattá válik. A RAM memória és tartalma, amíg a személyi számítógépek jelen lesznek mindennapi életünkben, jelentős bizonyítékforrásként fog rendelkezésre állni a nyomozási cselekmények során.

A felhőszolgáltatások széles körben való elterjedésének köszönhetően napjainkban könnyedén előfordulhat, hogy az elektronikus adatokat nem egy fizikai tárhelyen, például merevlemezen, hanem idegen tárhelyeken rögzítjük, az esetek többségében pedig nem tárolódnak le a számítástechnikai készüléken. Ezeknek a digitális adatoknak az elérhetősége korlátozott, megkeresés útján a tárhelyszolgáltató tudja hozzáférhetővé tenni a nyomozó hatóság számára az érintett adatállományt. Szerencsére a RAM memória kivételt képez, hiszen adattartalma nem helyettesíthető egy távoli szerver által, bizonyos munkafolyamatok pedig csak benne lelehetők fel, így a jövőre nézve szerepe nem fog háttérbe szorulni az operatív tárban található releváns adattartalom.

Napjainkban az operatív tár jelenléte nemcsak számítógépekben, laptopokban, mobiltelefonokban van jelen, hanem olyan eszközökben, mint az okoshűtők, okosporszívók, vagy az innovatív Athom Homey⁷⁴ otthoni központi vezérlőegység. Bár az említett elektronikai eszközök RAM adattartalmának jelentősége valószínűleg nem releváns bizonyítékforrás a rendvédelmi szervek számára, az a tendencia igen csak észrevehető, miszerint egyre több okoseszközben lelehető fel a RAM memória, mint fizikai alkotóelem.

⁷⁴ Athom Homey (<https://homey.app/en-us/homey/>) Megtekintve: 2021.10.06.

8. ÖSSZEGZÉS, HIPOTÉZISEK IGAZOLÁSA

A kutatásom és egyben a dolgozatom végéhez érve sorrendben értékelem az általam megfogalmazott hipotéziseket.

Az első feltevés, miszerint a RAM memória forenzikus vizsgálatához előzetes számítástechnikai jártasságokra van szükség, amely rövid időn belül elsajátítható oktatással és segédlettel, vizsgálataim szerint igaz állítás. A RAM mentéséből származó információk sok esetben azért nem tudnak a büntetőeljárásokban releváns szerepet játszani, mert a végrehajtó állomány nincs azon készségek birtokában, hogy azt sikeresen le tudja menteni. Az operatív tár adattartalmának a rögzítése egy egyszerű folyamat, mert a külső adathordozó fizikai alapon történő teljes törlésén és a memóriamentésre alkalmas szoftverrel való ellátása nem okozhat komolyabb fejtörést. Egyrészt a környezetnek a jelentős szerepe sem elhanyagolható, hiszen egyedi felhasználású személyi számítógépek, laptopok adatmentése egyszerű, és a végrehajtói állomány által végrehajtható. Másrészt a szerverkörnyezet, vagy titkosított meghajtók feloldása már szakértő vagy szaktanácsadó közreműködésével történik, amellyel a memóriamentési folyamat eredményessége nagyban biztosított, illetve az esetlegesen felmerülő problémákra azonnal képesek reagálni. Amennyiben megkapja a végrehajtó állomány a képzést és gyakorlattá válik a RAM memória rögzítése, akkor nagyobb arányban fog szerepet játszani a büntetőeljárásokban. A kriminalisztika kezdetén a vérgyanús szennyeződések sem rögzítették, aztán a vércsoport meghatározással, illetve a DNS-el már kihagyhatatlanná vált. Ellenben ahhoz, hogy a memória forenzikus vizsgálata célra vezetően, hatékonyan és a körülményekhez képest rövid időn belül végrehajtható legyen, már igazságügyi informatikai szakértő igénybevételével valósulhat meg. Nem véletlenül igényel különleges szakértelmet vagy szaktanácsadói kompetenciát a számítógépeken, laptopokon fellelhető elektronikus adatok külső helyszínen történő rögzítése, ami a gyakorlatban sokszor alakulhat úgy, hogy a nyomozó hatóság feladata, illetve a már megszerzett memóriakép laboratóriumban történő vizsgálata. A kimeneti eredményekben fellelhető releváns információk, kártékony programok kódjai illetve egyéb digitális bizonyítékok laikus szemmel nehezen észrevehetők még egy grafikus megjelenésű programban is, nemhogy egy parancssori segédprogramban.

A második feltételezésemben azt fogalmaztam meg, hogy a nyílt forráskódú programok nem képesek olyan mélységben digitális bizonyítékokat kinyerni egy memóriafájlból, mint a zárt forráskódú alkalmazások. A felvetésem hamis igazolást nyert. A parancssori megjelenésű

Volatility olyan részletes munkafolyamatok, hálózati kapcsolatok, rendszeradatok lekérdezésére is képes egy memóriaképből, ami eredményében számottevőnek bizonyul. Nem véletlenül alkalmazzák olyan nemzetközi szervezetek oktatási és gyakorlási célokra,⁷⁵ mint az ENISA. A letisztult grafikus felülettel rendelkező Redline-al olyan többletismeretek birtokába juthatunk, mint böngészési és letöltési előzmények. Az open source szoftvereknek kezelésének vannak bizonyos hátulütőik is, gondoljunk csak a Redline sajátos fájlrendszerére és a kizárólag Windows operációs rendszeren történő alkalmazására, illetve a Volatility esetében az utasítások karakterre pontos bevitelénél, ennek ellenére a hiteles nyílt forráskódú alkalmazások igenis képesek részletesen, alapjaiban a memóriakép adatállományából releváns adatokat kinyerni.

A harmadik hipotézisem arra irányult, hogy nem állítható fel egy egyértelmű rangsor a memória elemzésére megalkotott alkalmazások között számos tényezőnek köszönhetően. Tapasztalataim alapján ez egy igaz állítás. Minden alkalmazás alapjaiban különbözik egymástól. Van, amit nem fejlesztenek tovább, így csak régebbi operációs rendszerek memóriájának elemzésére szolgálnak, illetve a naprakész szoftverek szerkezete is megoszlik a parancssori és grafikus interfész között. A zárt forráskódú, nyomozó hatóságok számára rendelkezésre álló programok pedig rendelkezhetnek programhibákkal, amelyet a szoftverek időnkénti frissítésével igyekeznek kiküszöbölni. Ezt én személyesen is tapasztaltam a kutatásom során, amikor a Roast Lamb több órás elemzés után egy keresési kategóriát nem tudott lefuttatni, ami miatt lefagyott a művelet és kénytelenek voltunk újraindítani az egész vizsgálatot. Ahhoz, hogy melyik alkalmazást használjuk egy memóriaképen a minél részletgazdagabb keresési eredmények eléréséhez, szükséges múltbéli, vagy gyakorlati tapasztalattal rendelkezni, illetve tanulmányokat, útmutatókat, segédanyagokat tanulmányozni ahhoz, hogy kialakuljon az egyéni preferencia. Ráadásul egy adott szoftver nem biztos, hogy a vizsgáló által várt eredményeket produkálja. Megoldás lehet, hogy minél több alkalmazás álljon rendelkezésre a memóriaelemzéshez, így amennyiben az egyik nem alkalmas bűnügyileg releváns adatok kinyerésére, úgy könnyedén tudunk egy másikhoz nyúlni.

⁷⁵ Az ENISA honlapja: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1_forensic_analysis_i-handbook Letöltve: 2021.10.08.

9. ÁBRAJEGYZÉK

1. kép: FTK Imager report.....	21
2. kép: A Volatility kezelőfelülete	27
3. kép: Volatility 3 munkafolyamatok.....	28
4. kép: Redline főmenü	29
5. kép: Redline munkaablak.....	30
6. kép: Redline elemzési eredmények	30
7. kép: FTK Imager letöltése.....	31
8. kép: FTK Imager főmenü.....	32
9. kép: Belkasoft Evidence Center X	33
10. kép: Belkasoft Live RAM Capturer főmenü	34
11. kép: Belkasoft Evidence Center X munkafolyamatok	35
12. kép: Belkasoft Evidence Center X keresési eredmények.....	36
13. kép: Roast Lamb.....	37
14. kép: Roast Lamb főmenü	38
15. kép: Roast Lamb munkafolyamat	39
16. kép: Roast Lamb befejezett vizsgálat.....	39
17. kép: Roast lamb vizsgálati eredmények Excel-ben.....	40

10. IRODALOMJEGYZÉK

10.1. Szakirodalmak

1. Fehér Krisztián: Hackertechnikák: Útmutató valódi hacker módszerek biztonságos ki-próbálásához, BBS-INFO kiadó, 2018.
2. Fehér Krisztián: Számítógépvásárlási túlélőkönyv, szerzői magánkiadás, 2020
3. Gyaraki Réka – Simon Béla – Nagy Zoltán: Kiberbűncselekmények felderítése és nyomozása, In.: Kiss Tibor (szerk.) – Kibervédelem a bűnügyi tudományokban, Dialóg Campus, Budapest, 2020. (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf) [2021.06.08.]
4. Ivor Kollár: Forensic RAM dump image analyser, Univerzita Karlova, 2010, 6-7. o. (https://dspace.cuni.cz/bitstream/handle/20.500.11956/34206/DPTX_2007_1_11320_0_231778_0_48540.pdf?sequence=1&isAllowed=y) Letöltés ideje: 2021.05.13.
5. Máté István: A számítógép felépítése – Memóriák és csatlakozásuk. A BIOS., NSZFI, 2012, 6. oldal (https://www.academia.edu/1107969/Mem%C3%B3ri%C3%A1k_%C3%A9s_csatlakoztat%C3%A1suk_Working_with_computers_memory) Letöltve: 2021.11.02.
6. Mike Meyers: PC hardver és karbantartása, PANEM KFT, 2004
7. Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons, Inc., Indianapolis, Indiana, 2014, ([https://repo.zenk-security.com/Forensic/The%20Art%20of%20Memory%20Forensics%20-%20Detecting%20Malware%20and%20Threats%20in%20Windows,%20Linux,%20and%20Mac%20Memory%20\(2014\).pdf](https://repo.zenk-security.com/Forensic/The%20Art%20of%20Memory%20Forensics%20-%20Detecting%20Malware%20and%20Threats%20in%20Windows,%20Linux,%20and%20Mac%20Memory%20(2014).pdf)) Letöltés ideje: 2021.10.05.
8. Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények egyetemi jegyzet, Pécs, 2017.
9. Nagy Zoltán András (szerk.): Kibernyomozói kézikönyv. Szerzők: Halász Viktor, Herédi István, Gyaraki Réka, Kovács Zoltán, Máté István Zsolt, Nagy Zoltán András, Nagy Tamás, Simon Béla, In.: Ruzsonyi Péter (szerk.) – Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok III, Ludovika Egyetemi Kiadó, Budapest, 2020, https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/TKP_Kozbiztonsag.pdf [2021.05.13.]

10. Vassil Roussev: Digital Forensic Science: Issues, Methods, and Challenges, University of New Orleans, 2017.

10.2. Jogszabályok, rendeletek, módszertani levelek

1. 2017. évi XC. törvény a büntetőeljárásról (<https://njt.hu/jogszabaly/2017-90-00-00-11>)
Letöltés ideje: 2021.06.14.
2. 100/2018 (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól (<https://njt.hu/jogszabaly/2018-100-20-22>) [2021.09.07.]
3. 11/2003. (V. 8.) IM–BM–PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról (<https://njt.hu/jogszabaly/2003-11-20-06>) Letöltés ideje: 2021.09.14.
4. 2010 North Carolina Code Chapter 14 Criminal Law. Article 60 - Computer Related Crime (<https://law.justia.com/codes/north-carolina/2010/chapter14/article60/>) Megtekintve: 2021.09.20.
5. 2016. évi XXIX. törvény az igazságügyi szakértőkről (<https://njt.hu/jogszabaly/2016-29-00-00>) Megtekintve: 2021.09.20.
6. 9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről (<https://njt.hu/jogszabaly/2006-9-20-06>) Megtekintve: 2021.09.20.
7. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről (<https://njt.hu/jogszabaly/2013-25-20-0A>) Megtekintve: 2021.09.20.
8. 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (<https://njt.hu/jogszabaly/2004-79-00-00>) Letöltés ideje: 2021.09.21.
9. A Magyar Igazságügyi Szakértői Kamara 6/2020 számú Módszertani levele az elektronikus adatok vizsgálatának általános alapelveiről, 2020, (https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf) [2021.06.14.]
10. Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32013L0040>) Megtekintve: 2021.09.21.

10.3. Előadások, konferenciák

1. DFRWS. DFRWS 2005 forensics challenge, 2005. (<http://old.dfrws.org/2005/challenge/index.shtml>) Letöltés ideje: 2021.05.12.
2. Geiger, M., Venema, W., and Casey, E. DFRWS 2008 forensics challenge, 2008 (<http://old.dfrws.org/2008/challenge/index.shtml>) Letöltés ideje: 2021.05.12.

10.4. Internetes hivatkozások

1. Athom Homey (<https://homey.app/en-us/homey/>) Megtekintve: 2021.10.06.
2. Az ENISA honlapja: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1_forensic_analysis_i-handbook Letöltve: 2021.10.08.
3. Belkasoft Evidence Center X (<https://belkasoft.com/x>) Megtekintve: 2021.09.28.
4. Belkasoft Remote Acquisition (<https://belkasoft.com/r>) Megtekintve: 2021.09.30.
5. Boot Camp segédprogram (<https://support.apple.com/hu-hu/boot-camp>) [2021.10.02.]
6. CCleaner szoftver (<https://www.ccleaner.com/ccleaner/download>) [2021.09.20.]
7. FREETOOL – Free Reliable Tools for Investigating Cybercrime (<https://thefreetool-project.eu/>) Megtekintve: 2021.10.04.
8. LiME - Linux Memory Extractor (<https://github.com/504ensicsLabs/LiME>) [2021.10.05.]
9. Mac Memory Reader – MMR (<https://www.sans.org/blog/mac-os-forensics-how-to-simple-ram-acquisition-and-analysis-with-mac-memory-reader-part-1/>) [2021.10.05.]
10. Memory Forensics for Incident Response – Varonis (<https://www.varonis.com/blog/memory-forensics/>) Megtekintve: 2021.10.06.
11. Memoryze (macOS) (<https://fireeye.market/apps/211372>) Megtekintve: 2021.10.05.
12. Microsoft AVML – Acquire Volatile Memory for Linux (<https://github.com/microsoft/avml>) Megtekintve: 2021.10.05.
13. Oracle VM VirtualBox (<https://www.virtualbox.org/>) Megtekintve: 2021.09.22.
14. OSXPmem – Mac OS X Physical Memory Acquisition tool (<https://code.google.com/archive/p/pmem/wikis/OSXPmem.wiki>) Megtekintve: 2021.10.05.
15. Python <https://www.python.org/> Megtekintve: 2021.09.25.
16. Python PE elemző modul <https://pypi.org/project/pefile/> Megtekintve: 2021.09.25.
17. Rekall Forensics <http://www.rekall-forensic.com/home> Megtekintve: 2021.09.26.

18. Rushita Dave, Nilay R. Mistry, M. S. Dahiya: Volatile Memory Based Forensic Artifacts & Analysis, Gujarat Forensic Sciences University, 2014, (<https://cyberforensicator.com/wp-content/uploads/2018/02/fileserve.pdf>) [2021.10.06.]
19. VMware Workstation Player (<https://www.vmware.com/products/workstation-player.html>) Megtekintve: 2021.09.22.
20. Volatility Foundation (<https://www.volatilityfoundation.org/>) [2021.09.22.]
21. WinPmem (<https://github.com/Velocidex/WinPmem>) Megtekintve: 2021.09.22.

11. MELLÉKLETEK

11.1. A teljes anonimizált esettanulmány

A SZAKÉRTŐ KIRENDELÉSE

A Budapesti Rendőr-főkapitányság, ×××. kerületi Rendőrkapitányság vezetője a 01×××/××××/2020.bü. számú ügyben 2020. december ××.-n szakértő kirendeléséről határozott. A határozatában rögzített adatok vizsgálatára és a feltett kérdések megválaszolására a Nemzeti Szakértői és Kutató Központot rendelte ki igazságügyi szakértői vélemény előterjesztésére.

A NSZKK ×××××× Intézetének vezetője ×××××× ×××××× igazságügyi informatikai szakértőt jelölte ki a szakvélemény elkészítésére. A kirendelt szakértő jelen üggyel kapcsolatban

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
- informatikai rendszerek tervezése, szervezése,
- informatikai biztonság

szakterületeken jogosult szakvéleményt adni.

I. ELŐZMÉNYEK

A fenti bűnügyi szám alatt a Büntető Törvénykönyvről szóló 2012. évi C. törvény 204. § (1) bekezdés a) pontjába ütköző és az (1) bekezdés a) pontja szerint minősülő tizennyolcadik életévét be nem töltött személyről, személyekről pornográf felvétel megszerzésével vagy tartásával elkövetett gyermekpornográfia büntettének megalapozott gyanúja miatt indult ügyben az eljáró hatóság informatikai eszközöket foglalt le, amely vizsgálata szükséges az ügy szempontjából lényeges tények megállapítására.

II. A SZAKÉRTŐ FELADATA

A nyomozás során lefoglalt eszközök vizsgálata.

A kirendelő határozatban szereplő kérdések megválaszolása.

A kérdések a vélemény VI. fejezetében kerültek feltüntetésre.

V. SZAKMAI TÉNYMEGÁLLAPÍTÁSOK

1. Lenovo Thinkpad vizsgálata

A vizsgált számítógép (Lenovo P52 20MA-S1720B, sn: ××××××) egyetlen adathordozót (Samsung MZ-VLB512, sorozatszám ××××××) tartalmaz. Az adathordozó a gyártói teszt eredménye alapján hibamentes.

Az adathordozó teljes terjedelme alapján készített SHA1 hash-kulcs:

0c8f9687ffe7bde4199a7cfc3dacfe6df0××××××

Az adathordozón található fájlrendszert tartalmazó logikai egységek (partíciók):

Jelölés	Méret (GB)	Fájlrendszer	Kötet címke	Szabad terület (GB)
P1	0,75	FAT32	Boot	0,72
P2	0,02	MS Reserved	-	0,02
P3	471	NTFS Bitlocker	Windows	312
P4	4,8	NTFS	Recovery	4,3

A P1, P2, P4 partíciók az operációs rendszer helyreállításához szükséges állományokat tartalmazák.

A P3 partíció Bitlocker titkosítással védett. A titkosítás feloldásához szükséges helyreállító kulcs a vizsgálat során nem állt rendelkezésre. Az eredeti adathordozóról teljes értékű fizikai másolat készült egy típusazonos adathordozóra. A másolat a vizsgált számítógépbe beépítésre került. A számítógép bekapcsolásra került, a kirendelő által biztosított felhasználói adatok segítségével az operációs rendszerben létrehozott felhasználói fiók betöltésre került. A működő operációs rendszer által használt memóriáról (RAM) memóriakép készült, amely alapján a Passware Kit Forensic eszköz segítségével a titkosításhoz használt helyreállító adatok kiolvashatók voltak:

- BitLocker VMK: dalo4Zr8SvZy55fvsNH6zt/H68PikUVND6pauP××××××
- Recovery Key: 278190-009141-206767-536140-106524-019932-020086-××××××
- ID: 559A2A98-F0E9-4FD8-9F19-316F9B××××××

A kiolvasott Recovery Key segítségével a partíción tárolt adatok vizsgálhatók voltak

A P3 partíción („C”) található fájlok alapján megállapítható, hogy a partíció feltelepített operációs rendszert tartalmaz.

Az operációs rendszer adatai a beállításjegyzék alapján:

Típus:	Microsoft Windows 10
Regisztrált tulajdonos neve:	USER
Termékazonosító:	00330-80000-00000-AA041
Termékkulcs:	TY4CG-JDJH7-VJ2WF-DY4X9-×××××
Számítógép neve:	DESKTOP-QQK559Q
Utolsó használat ideje:	2020.11.20. 11:43
Telepítés időpontja:	2020.10.05. 9:45

Az operációs rendszerben az alapértelmezett fiókokon kívül helyi felhasználói fiók nem került létrehozásra, tartományi fiókként „gabor××××” felhasználó volt regisztrálva.

Az ügyel kapcsolatba hozható felhasználói állományok a P3\Users\gabor×××× mappán belül voltak fellelhetők. A felhasználói állományok másolata adathordozón csatolásra került. A felhasználói állományok egy része munkavégzéssel kapcsolatos, üzleti titkot képezhetnek.

A Downloads mappában egy darab szexuális tartalmú kép (117174983_2372164936426595_5536512723606653093_n.png) volt fellelhető. A fájl attribútumok alapján megállapítható, hogy a fájl nagy valószínűséggel 2020.08.07 20:49-kor került letöltésre a számítógépre. A képet készítő eszközről, a kép készítésének körülményeiről nem áll rendelkezésre információ.

A tárolt böngészési előzmények és böngészőkben tárolt felhasználói adatok alapján készített kimutatások adathordozón csatolásra kerültek.

A számítógépen munkavégzéshez szükséges szoftverek voltak fellelhetők.

A helyreállítható, korábban törölt állományok adathordozón csatolásra kerültek.

11.2. Segédlet a számítógépek, laptopok közvetlen hozzáférésű memóriájának (RAM) lementéséhez és forenzikus vizsgálatához

KÉPEK JEGYZÉKE

1. kép: Számítógép névjegye.....	59
2. kép: CCleaner letöltése.....	60
3. kép: Drive Wiper	61
4. kép: USB-meghajtó formázása.....	62
5. kép: Belkasoft Live RAM Capturer igénylése	63
6. kép: RAM Capturer letöltési hivatkozás	63
7. kép: FTK Imager igénylése	65
8. kép: Adatmentésre alkalmas külső adathordozó	66
9. kép: RAM Capturer főmenü.....	67
10. kép: Mentett memóriakép.....	68
11. kép: FTK Imager.exe.....	69
12. kép: Forrás kiválasztása	70
13. kép: AD1 konténerfájl opció	70
14. kép: Konténerfájl létrehozása.....	71
15. kép: A konténerfájl adatai	71
16. kép: Konténerfájl könyvtára.....	72
17. kép: Konténerbe helyezés megerősítése.....	73
18. kép: Konténerbe helyezési folyamat	73
19. kép: Konténerfájl hash-kulcsai.....	74
20. kép: A konténerfájl könyvtára.....	75
21. kép: Memóriakép kicsomagolása	76
22. kép: Konténerfájl kiválasztása	77
23. kép: Memóriakép kicsomagolása	78
24. kép: Memóriakép kicsomagolási folyamat	78
25. kép: Roast Lamb főmenü	79
26. kép: Ritka blokkok felmérése.....	79
27. kép: Roast Lamb munkafelület	80
28. kép: Roast Lamb munkafolyamatok	81
29. kép: Roast lamb munkafolyamat befejezése	81
30. kép: Keresési eredmények helye	82

31. kép: Vizsgálati eredmények megtekintése	82
32. kép: Eredmények Excelben.....	83

1. BEVEZETÉS

A Tudományos Diákköri dolgozatom elkészítésekor arra törekedtem, hogy közérthető megfogalmazással minél részletesebben mutassam be a számítógépek, laptopok közvetlen hozzáférésű memóriájának (a továbbiakban: RAM) forenzikus vizsgálatát, illetve annak gyakorlati szempontjait. Annak érdekében, hogy a végrehajtó állomány következetesen, pontosan, eredményesen hajtsa végre a mentési és vizsgálati folyamatokat, célszerűnek tartottam egy olyan útmutatót készíteni, amelyben én magam fogom végrehajtani a dolgozatomban már ismertetett számítástechnikai műveleteket lépésről-lépésre, pontosan, fényképfelvételekkel illusztrálva.

A gyakorlati feladat viszonylag kevés feladat végrehajtásából áll, de időigényes, mert az egyes lépéseknél a számítógépnek vagy laptopnak akár több órán keresztül kell lefuttatnia. Mellette más munkamenetet sokszor nagyon lassan vagy nem végez el az eszközünk, köszönhetően az erőforrásigényes eljárásoknak. Munkaigényesség szempontjából hamar konstatálható, hogy nem okoz komolyabb fejtörést a memóriamentési és elemzési folyamat, mégis készségszinten kevés felhasználó rendelkezik a megfelelő képzettséggel.

Az alábbi esettanulmányban azt modellezem, hogy egy bűnügyi nyomozó előkészít egy adathordozót külső helyszínen történő adatmentésre, majd a helyszínen a kérdéses személyi számítógép, laptop RAM memóriáját lementi úgy, hogy az elektronikus adat változatlansága a büntetőeljárás során ne legyen megkérdőjelezhető. Praktikusság szempontjából célszerű pendrive-ot alkalmazni, mint ahogy magam is fogom tenni, de egy külső merevlemez is megfelelő.

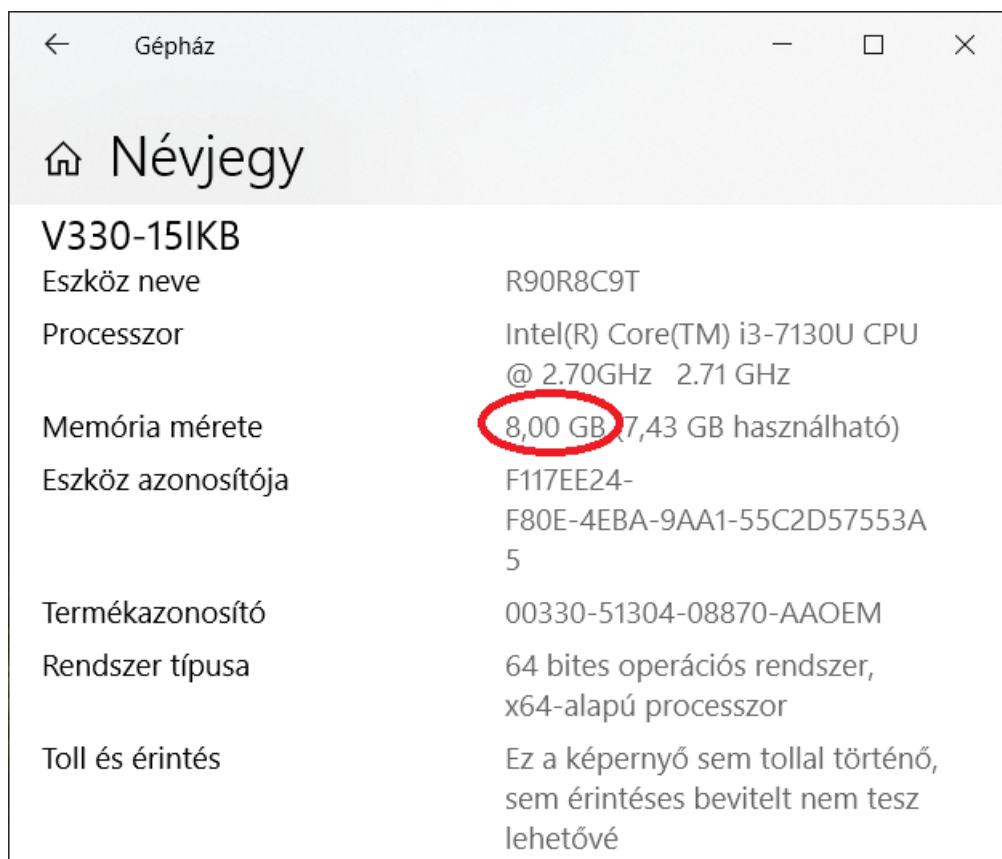
Fontosnak tartom megjegyezni, hogy jelen segédlet kizárólag a személyi használatú, Windows operációs rendszerek 32 és 64 bites verziójának memóriájának lementésére és vizsgálatára szolgál, köszönhetően a Windows dominanciájának és népszerűségének. Szerverkörnyezetben történő adatmentés, vagy titkosított meghajtók feloldása igazságügyi informatikai szakértői vagy szaktanácsadói kompetencia, amely túlmutat a segédanyag ismertetési céljain. Amennyiben előzetesen rendelkezésre állnak olyan információk, miszerint a külső helyszínen történő adatmentés során informatikában jártasabb felhasználók számítástechnikai eszközén kell az adatmentést végrehajtani, célszerű szakértőt vagy szaktanácsadót bevonni a folyamatok eredményes lefolytatásához és az esetlegesen felmerülő problémák kiküszöbölésére.

Az útmutatóban a Belkasoft Live RAM Capturer, az Accessdata FTK Imager és a Roast Lamb alkalmazást fogom igénybe venni, amelyekről részletesebben a tudományos diákköri dolgozatomban olvashatunk, egy Windows 10 Pro 64-bites operációs rendszeren.

2. A KÜLSŐ ADATHORDOZÓ KIVÁLASZTÁSA, ELŐKÉSZÍTÉSE

Első lépésként egy pendrive-ot fogok behelyezni a számítógémem külső csatlakozójába, amely nagyobb tárhellyel rendelkezik, mint amekkora RAM memória található a számítógépben, laptopban. Célszerűségi szempontból érdemes USB 3.0 vagy annál gyorsabb választani, amellyel időt spórolhatunk meg. Pendrive esetében minimum 32 vagy 64 GB-os, esetleg ennél nagyobb tárhelyű eszközt használjunk, de ez függhet számos tényezőtől. Előzetes ismeret birtokában egyszerűbb a kiválasztás, illetve saját vagy külső eszközön néhány kattintás alatt megtekinthető a RAM mérete.

Windows 10 esetében: Start menü → Gépház/Vezérlőpult → Rendszer → Névjegy, de egyébként a Fájlkezelőben is meg tudjuk tekinteni a „Rendszer tulajdonságai” menüpontban.



18. kép: Számítógép névjegye
Forrás: a szerző

Napjainkban azért a személyi használatú számítógépek operatív tárja felhasználótól függően jellemzően 4 GB, 8 GB vagy 16 GB tárhelyű körül határozható be. Lehetőség szerint

több, különböző tárhelyű, nyomozó hatású által biztosított pendrive, vagy egy nagyméretű külső merevlemez álljon rendelkezésre a helyszínen.

2.1. Az adathordozó előkészítése

Ebben a szakaszban előkészítünk egy pendrive-ot a helyszíni RAM memória rögzítésére.

A már előkészített üres adathordozót nem elég egyszerű gyorsformázással felkészíteni a külső adatmentésre, hanem szükséges bitről-bitre átírni a tárhelyét. Ezzel kiküszöbölhetjük azt, hogy az eljárás szempontjából nem releváns digitális adat marad az adathordozón. Ezt a folyamatot nevezzük „wipe”-olásnak. Számtalan módon megvalósítható, de a legegyszerűbb és leggyorsabb módszere az ingyenes „CCleaner” nevű alkalmazás segítségével végrehajtható.

A www.ccleaner.com oldalon a „Download” fül alatt megtalálható „Download CCleaner” menüpontra kattintva az oldal alján letölthető az ingyenes, nyílt forráskódú verziója.

Software Updater Quickly updates apps to reduce security vulnerabilities	✗	✓	✓
Cleans Everywhere Even places other cleaners can't reach	✗	✓	✓
Guards Against Junk Files Monitors junk in real-time	✗	✓	✓
Automatically Clears History Cleans your browser when you close it	✗	✓	✓
Faster, Longer-lasting Hard Drives Includes Defragger, to keep hard disks healthy and running efficiently			✓
File Recovery Includes Recuva, so you never have to worry about losing a file again			✓
See Inside your PC Includes Speccy, so you can spot issues or find compatible upgrades			✓
	Free Download	Buy Now \$29.95 \$24.95	Buy Now \$44.95 \$39.95

19. kép: CCleaner letöltése

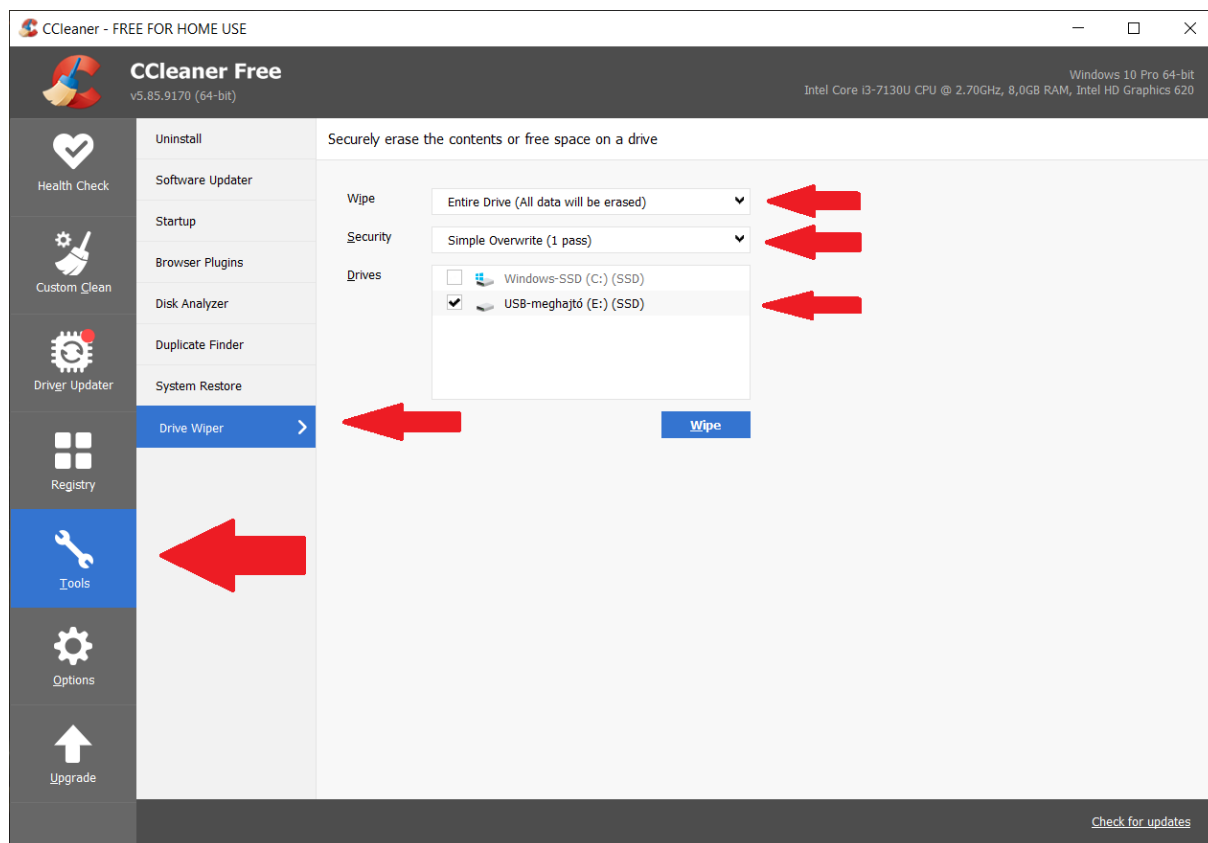
Forrás: a szerző

A letöltést követően egy egyszerű telepítési folyamatot kell megerősítenünk, majd az alkalmazás használatra készvé válik.

A megnyitását követően a „Tools” menüpontra kattintva, majd a legutolsó „Drive Wiper” modult kiválasztva beállítjuk, hogy ne csak az üres tárterületet, hanem az egész adathordozó

adattartalmát törölje (Entire Drive). Az egyszeri felülírás, azaz „Simple Overwrite (1 pass)” elegendő, majd kiválasztjuk a meghajtót, ami az én esetemben az „USB-meghajtó (E:)”.

Kiemelten fontos, hogy megfelelő mezőt jelöljünk ki, mert a másik meghajtó törlése visszavonhatatlan destruktív folyamat. A „Wipe” gombra kattintva (majd utána begépelve az „ERASE” parancsot) megkezdődik a fizikai adathordozó teljes adattartalmának a törlése.

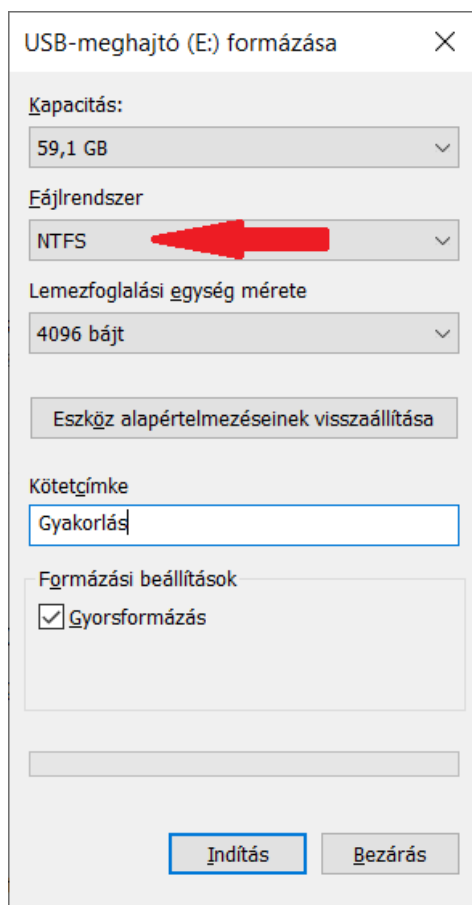


20. kép: Drive Wiper
Forrás: a szerző

A pendrive, vagy más külső adathordozó esetében a felülírási folyamat eltérő, amely függ az adathordozó tárhelykapacitásától. Az én esetemben egy 60 GB méretű pendrive-ot közel másfél óra leforgása alatt vitte véghez a törlési folyamatot.

A fájlrendszer szintén fontos szerepet játszik egy pendrive formázása során. Amennyiben „FAT32” a fájlrendszer, azt egy gyorsformázással szükséges „NTFS”-re állítani, mert a FAT32 mindössze 2 GB méretű fájlokat képes fogadni és tárolni, míg az NTFS bármekkora. Márpedig a RAM memória ennél szinte mindig nagyobb méretű. Ezt ellenőrizni a fájlkezelőben tudjuk, jobb egérgombbal kattintva az USB meghajtón a „Tulajdonságok” fülre kattintva láthatóvá válik a pendrive mérete, fájlrendszere.

Formázni az USB-meghajtót a jobb egérgomb, majd „Formázás” földre kattintva lehetséges. Itt a kötelező elem a Fájlrendszer kiválasztása, ami értelemszerűen „NTFS” lesz. Megnevezést, azaz Kötetcímkét szabadon beállíthatunk, majd az „Indítás” gombra kattintva néhány másodperc alatt befejeződik a formázás. Mivel korábban a CCleanerrel teljesen lewipeoltuk az adathordozót, ezért jelen esetben a gyorsformázás elegendő. Amennyiben alapból NTFS a pendrive vagy külső merevlemez fájlrendszere, az említett lépés kihagyható.



21. kép: USB-meghajtó formázása
Forrás: a szerző

Most, hogy rendelkezésünkre áll egy teljesen wipe-olt pendrive, amely az NTFS fájlrendszerrel képes 2 GB-nál nagyobb fájlokat fogadni, következő előkészületi lépésként rá kell helyoznunk egy olyan RAM memóriamentésre szolgáló alkalmazást, amely telepítési folyamat nélkül képes a memória adattartalmat rögzíteni Windows 32 és 64 bites operációs rendszerek-nél. Éppen ezért a Belkasoft Live RAM Capturer nevű alkalmazást fogom használni.

A Belkasoft Live RAM Capturer letölthető a <https://belkasoft.com/> oldalról a „Download” földre kattintva, a megfelelő alkalmazást kiválasztva és az e-mail címünk bevitelével igényelhetünk a „Proceed” ikonnal.

22. kép: Belkasoft Live RAM Capturer igénylése
Forrás: a szerző

Fontos, hogy az e-mail fiókunk valós legyen, ne fiktív, mert a Belkasoft személyzete oda fogja kézbesíteni a letöltési linket az alkalmazáshoz, amely hozzávetőlegesen csak néhány napig érvényes. Miután megérkezett az e-mail, a benne szereplő hivatkozásra kattintva letöltődik a RAM Capturer program.

23. kép: RAM Capturer letöltési hivatkozás
Forrás: a szerző

Az alkalmazás „portable” verzió, amely nem igényel telepítést és ennek köszönhetően egyszerűen lehet alkalmazni külső helyszínen történő adatmentésre. A tömörített fájl kicsomagolását követően egy „x86” és egy „x64” mappa látható. Az x86 a 32 bites, míg az x64 a 64 bites operációs rendszerrel ellátott számítógépek, laptopok RAM memóriájának rögzítésére szolgál. Napjainkban a 64 bites operációs rendszerek dominálnak már a készülékeken, de célszerű mind a kettő mappát a wipe-olt adathordozóra áthelyezni, amellyel biztosítható az eredményes memóriamentési folyamat.

Végül, de nem utolsósorban, letöltjük az FTK Imager-t a pendrive-ra, amelynek segítségével konténerfájlba csomagoljuk a memóriaképet, majd hash-kulccsal ellátjuk egy későbbi folyamat során.

A <https://accessdata.com/> weboldalon a „Products & Services” fület lenyitva az „FTK Imager”-re, majd az átirányított weblapon a „Download FTK Imager” ikonra kattintunk. Ezt követően szükséges pár mezőt kitölteni az FTK Imager igényléséhez, viszont itt elegendő szintén csak az e-mail címünknek valódinak lennie, a többi adatnak pedig fiktívnek, hiszen az e-mail fiókunkra érkezik a letöltési hivatkozás, akárcsak a Belkasoft Live RAM Capturernél. Az „Email Opt In” mezőt kipipálva, majd a „Submit” gombra kattintva körülbelül negyed órán belül megérkezik a letöltési link a programhoz.

The image shows a registration form for FTK Imager. The form includes the following fields and options:

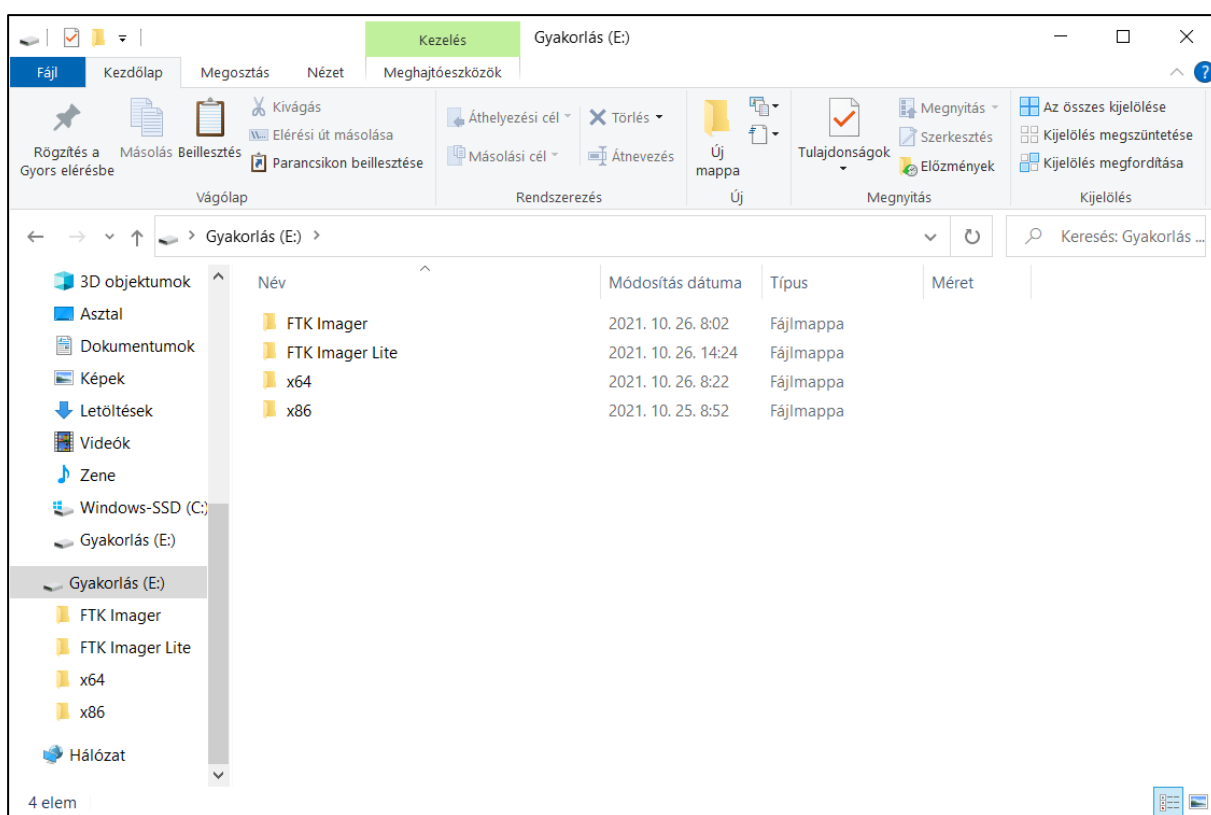
- Email:** talosadam13@gmail.com (indicated by a red arrow)
- Phone:** 06301234567
- Country:** Hungary (dropdown menu)
- Organization:** -
- Job Title:** -
- Job Function:** Other (dropdown menu)
- Organization Type:** Education (dropdown menu)
- My organization is currently using FTK:** Yes (dropdown menu)
- Email Opt In:** ☒ Yes* (indicated by a red arrow)
- SUBMIT** button (indicated by a red arrow)

24. kép: FTK Imager igénylése
Forrás: a szerző

A letöltést követően egy egyszerű telepítési folyamatot szükséges lefuttatni, amelyben elfogadásra kerülnek a felhasználási feltételek, és kijelölésre kerül egy könyvtár, ahova települ a program. Rövid idő alatt lefut a művelet, majd ezután az „Accesdata” mappán belül az „FTK Imager” mappát másoljuk át a wipe-olt pendrivera.

Ugyanezzel az eljárással az FTK Imager „Lite” verziója is letölthető, amely egy régebbi kiadás és a 32 bites operációs rendszerek memóriájának rögzítésére szolgál, míg az FTK Imager alapvetően a 64-es architektúráknál alkalmazható. Érdekesnek tartom letölteni mindkét alkalmazást, majd egy áthelyezni a wipeolt külső adathordozóra, ezzel garantálva a mentési folyamat eredményességét. Amennyiben a vizsgálandó számítógép operációs rendszere 64 bites, úgy az FTK Imagerrel is elvégezhető a memóriamentés a „File” fül „Capture memory” funkciójával.

Ezzel elértünk egy olyan állapotot, amely során a pendriveunk biztonságosan tud digitális nyomokat rögzíteni például egy kutatás vagy szemle során, majd azokat konténer fájlba hitelesíteni.



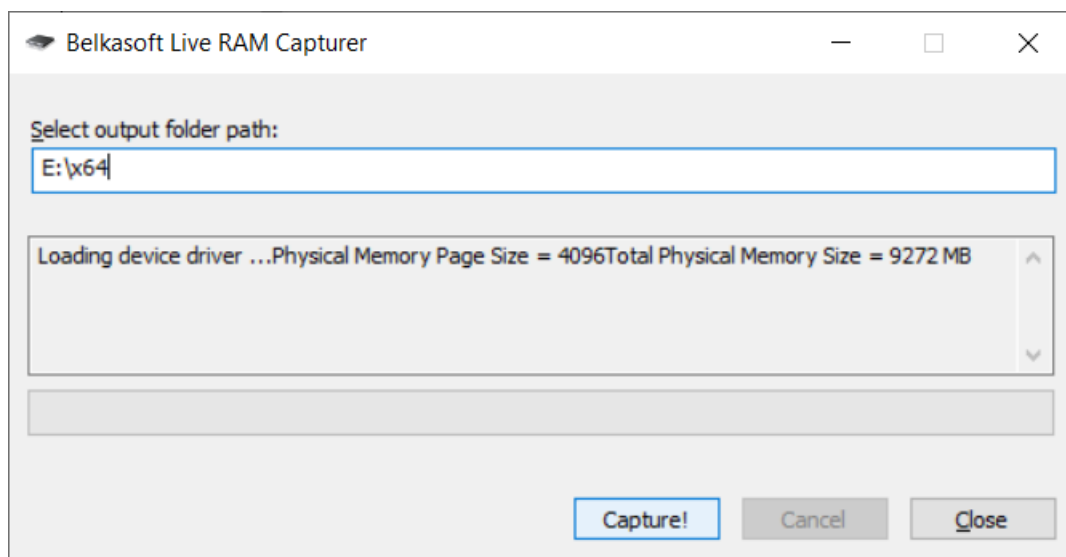
25. kép: Adatmentésre alkalmas külső adathordozó
Forrás: a szerző

3. A RAM MEMÓRIA MENTÉSE

Most azt fogjuk körbejárni, hogy milyen módon lehetséges a RAM memória rögzítése egy külső helyszínen működésben lévő Windows számítógépen, laptopon.

Erre a folyamatra azért van szükség, mert a RAM-ban tárolt elektronikus adatok a számítógép, laptop kikapcsolásával elvesznek. Így nem lehetséges lemodellezni, hogy a kikapcsolást megelőzően milyen alkalmazások futottak a készüléken, milyen bejelentkezések vagy kártékony kódok voltak rajta, stb. Egy memória mentést, azaz „memory dump”-ot fogunk készíteni.

A korábban említett lépésnek megfelelően leellenőrizhető, hogy a vizsgálandó számítógép operációs rendszere hány bites. Az én készüléken architektúrája 64 bit, tehát az „x64” mappát megnyitva lefuttatom a „RamCapture64” alkalmazást.

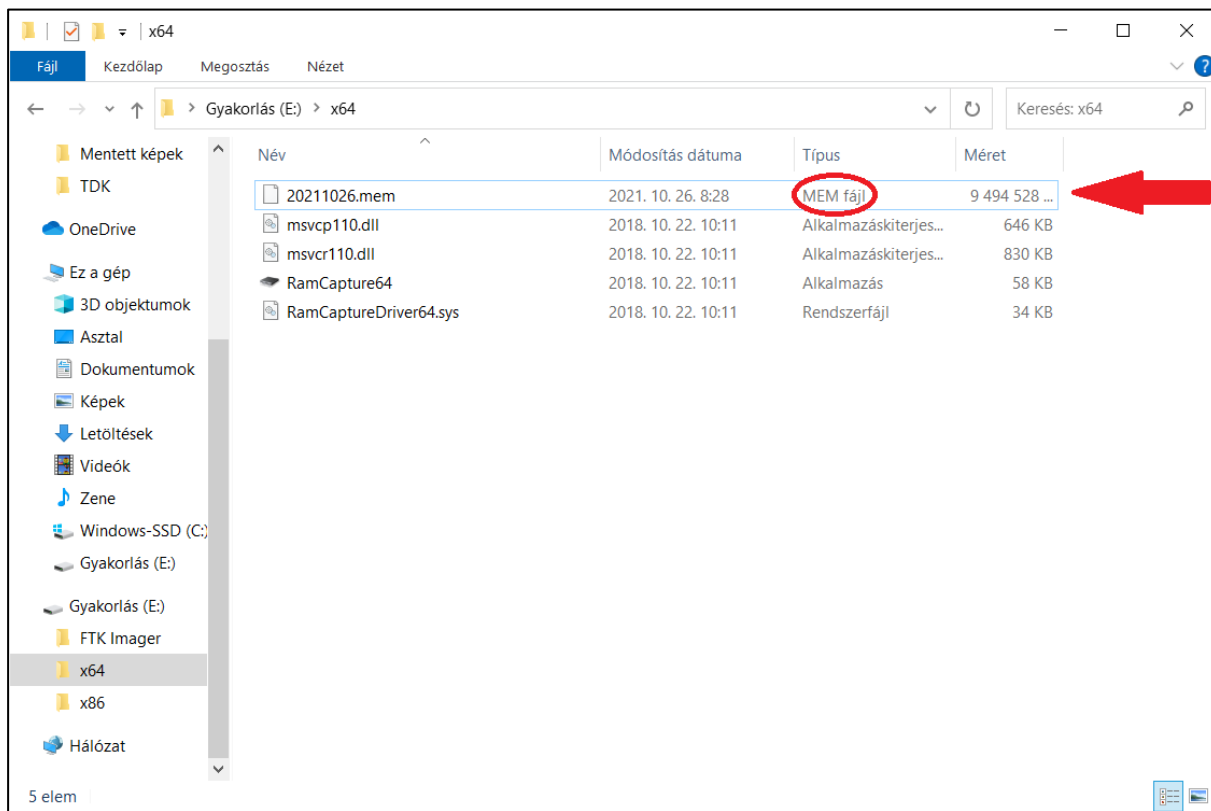


26. kép: RAM Capturer főmenü
Forrás: a szerző

A kimeneti eredmények mappa kapcsán győződjünk meg róla, hogy a külső adathordozó van megadva, majd a „Capture!” gombra kattintva ésszerű időn belül megtörténik a RAM adattartalmának rögzítése. Miután lefutott a folyamat, bezárhatjuk az alkalmazást. Az én esetemben az x64 mappán belül jött létre a memóriakép, amely megnevezése automatikusan a mai dátum.

Amennyiben nem a külső pendriveunkat, hanem a lefoglalandó gép merevlemezére hajtjuk végre a memória mentését, azzal a művelettel könnyen lehet, hogy törölt, de még nem felülírt területeket írunk át és ezzel az esély megszűnik, hogy arról a felületről bármi kinyerhető legyen olyan célszoftverekkel, mint az FTK.

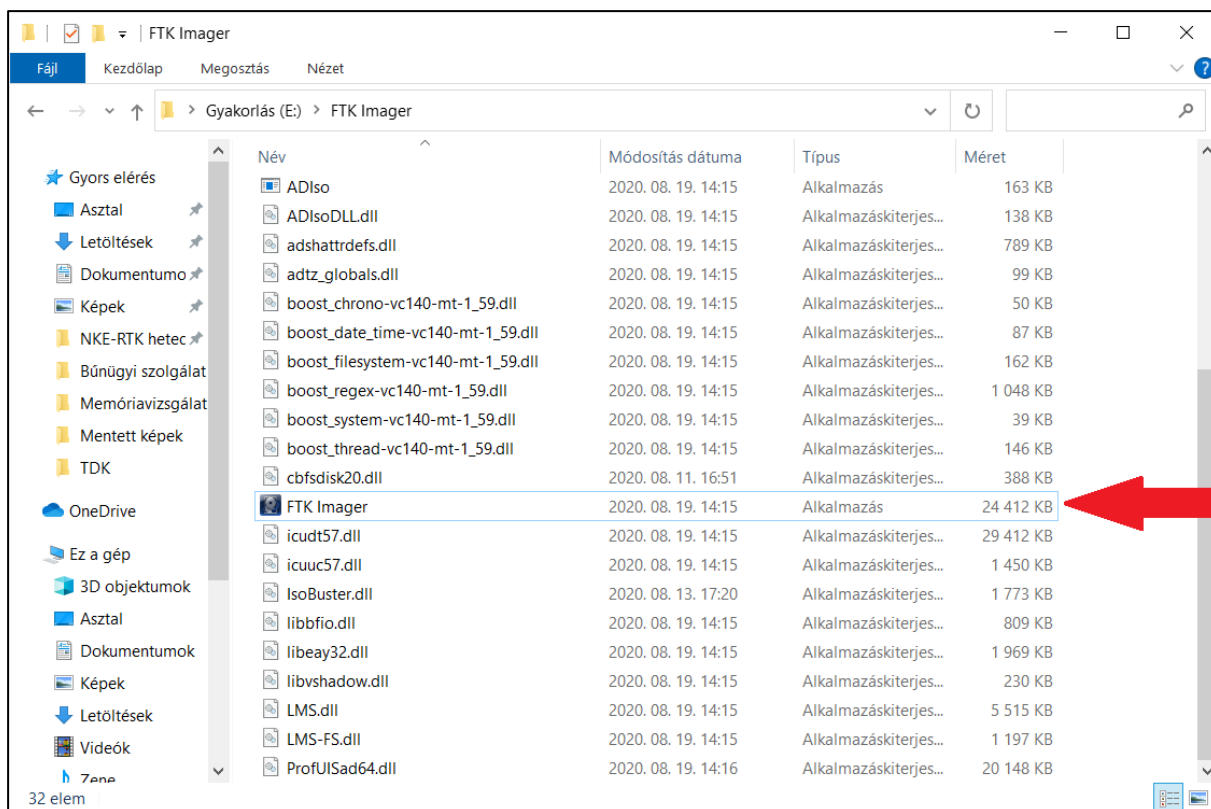
Ekkor egy „.mem” kiterjesztésű fájlt kapunk, amellyel külső helyszínen egy dolgunk maradt hátra, mégpedig konténer fájlba helyezni és jegyzőkönyvbe rögzíteni.



27. kép: Mentett memóriakép
Forrás: a szerző

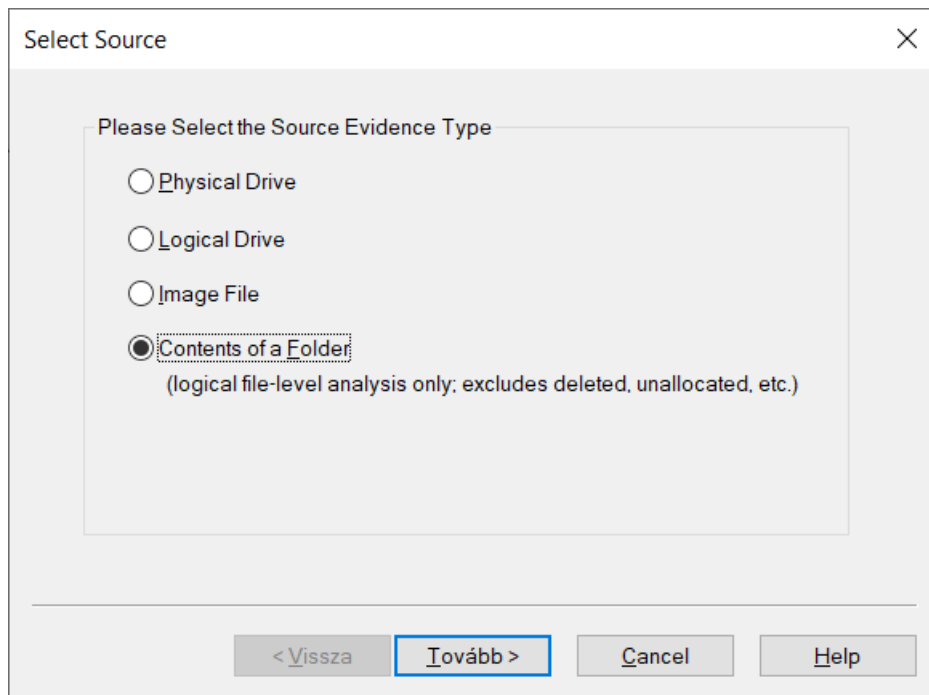
3.1. A memóriakép hitelesítése

A külső helyszínen végzett utolsó eljárási cselekmény, amelyet le fogok modellezni, a RAM memóriáról rögzített adattartalom hash-kulcsának kiszámítása, majd jegyzőkönyvben rögzítése. Ennek köszönhetően a büntetőeljárás során nem válik megkérdőjelezhetővé a lefoglaláskor rögzített memóriakép integritása. Ez konténerbe helyezéssel valósítható meg, amelyhez szükségünk lesz az FTK Imager alkalmazásra, amelyet a pendrive-on az FTK Imager mappán belül megnyitunk. Amennyiben egy 32 bites számítógépről történt a memóriamenési folyamat, annak megfelelően az FTK Imager Lite alkalmazást szükséges megnyitni, ellenkező esetben akadályok merülhetnek fel.



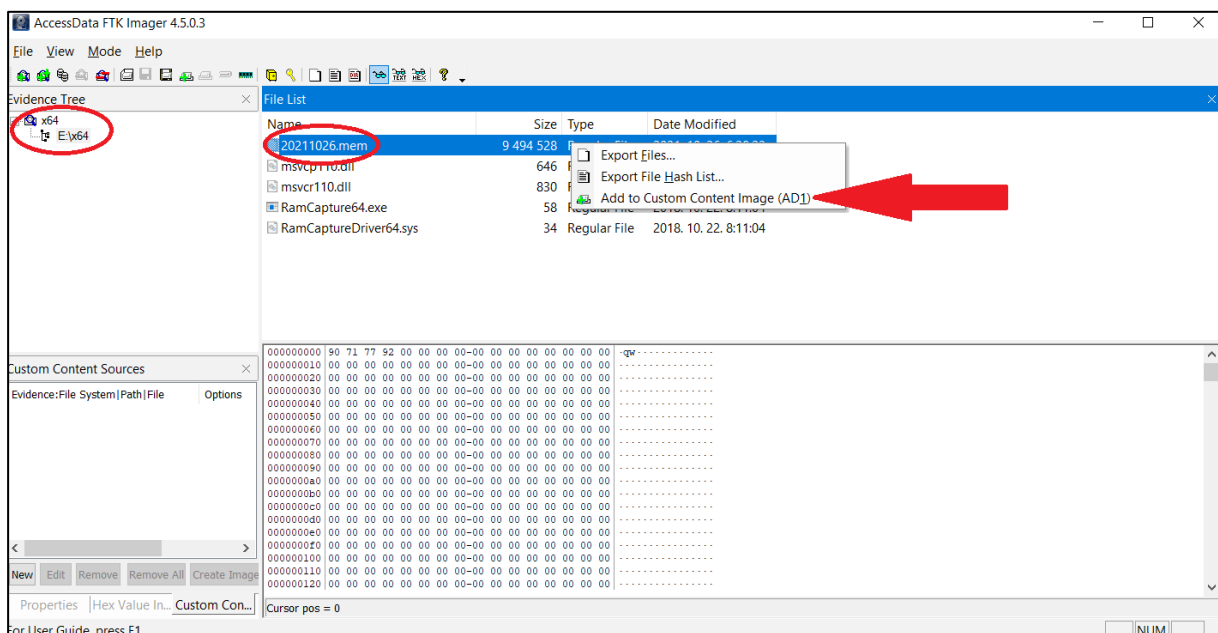
28. kép: FTK Imager.exe
Forrás: a szerző

A megnyitást követően a bal felső sarokban a „File” fület lenyitva rögtön az első találatra, az „Add Evidence Item” menü használatával egy új ablak jelenik meg, amelyben forrásként a memóriaképet kell megadnunk a „Contents of a Folder” mezőt bejelölve, majd kitallózzuk a memóriakép mentési helyét, ami az én esetemben az (E:) meghajtón az „x64” mappán belül található.



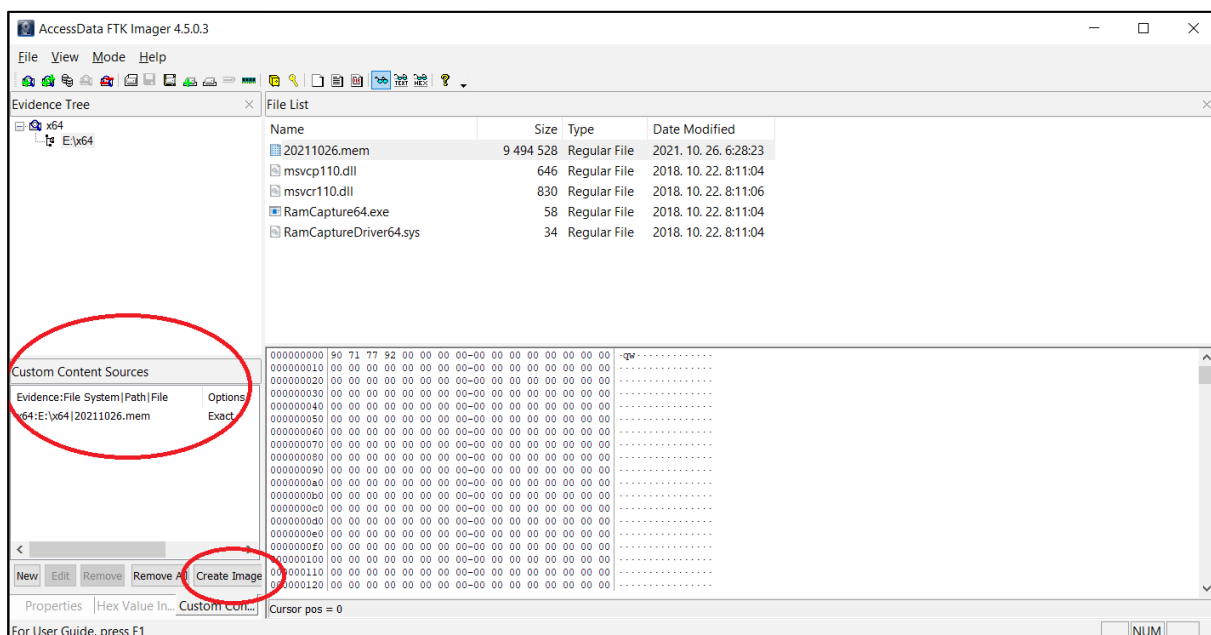
29. kép: Forrás kiválasztása
Forrás: a szerző

A „Finish” gombra kattintva a bal felső sarokban az „Evidence Tree” elnevezésű oszlopba megjelenik a kiválasztott mappánk. Duplán kattintva rá kicsomagolásra kerül az adathordozó adattartalma. Innen a „mem” kiterjesztésű állomány fog nekünk csak kelleni, amely könnyedén felismerhető a nagy méretéről. Jobb egérgombbal kattintva rá kiválasztjuk a harmadik opciót, az „Add to Custom Content Image (AD1)” lehetőséget.



30. kép: AD1 konténerfájl opció
Forrás: a szerző

Ezek után a bal alsó sarokban található „Custom Content Sources” mező alatt megjelenik a memórafájl. Itt a „Create Image” ikonra kattintva. Lehetséges, hogy ez az opció csak akkor látszik, ha teljes képernyős méretre van állítva az FTK Imager. Győződjünk meg róla.



31. kép: Konténerfájl létrehozása
Forrás: a szerző

A felugró ablakban az „Add” gombra kattintva tetszőlegesen kitölthetjük a megjelenő mezőket.

Evidence Item Information

Case Number:

Feladat

Evidence Number:

első

Unique Description:

gyakorlás

Examiner:

Minta János

Notes:

memóriakép

< Vissza

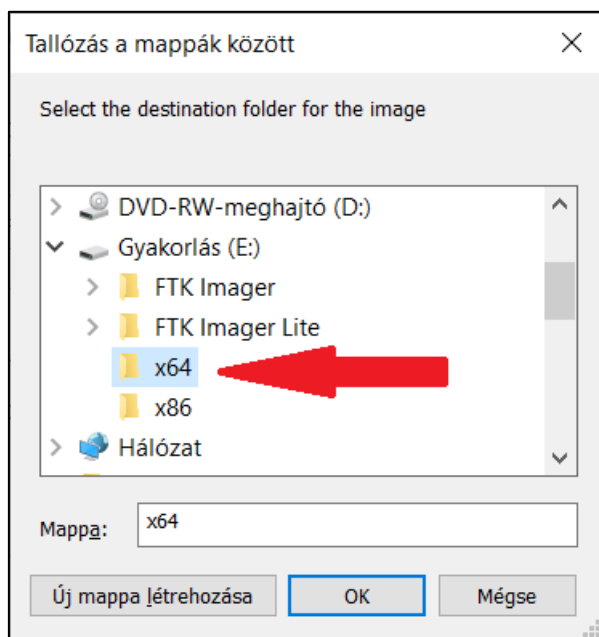
Tovább >

Cancel

Help

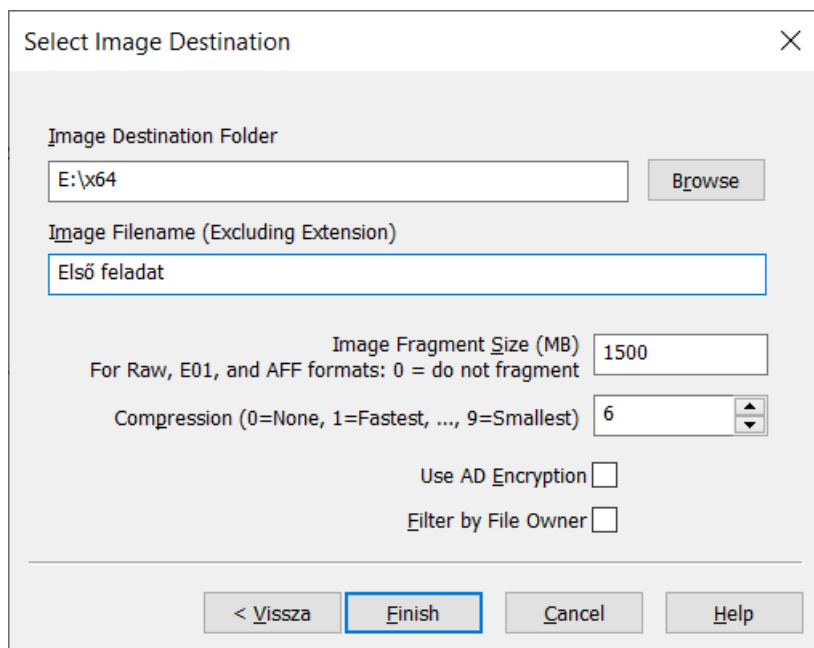
32. kép: A konténerfájl adatai
Forrás: a szerző

A „Tovább” gombra kattintva kijelölhetjük a mentési könyvtárat, amelynek kötelező minden esetben a külső adathordozónak lennie. Az én esetemben az „x64” mappa lesz, mert abban van a lementett memóriakép.



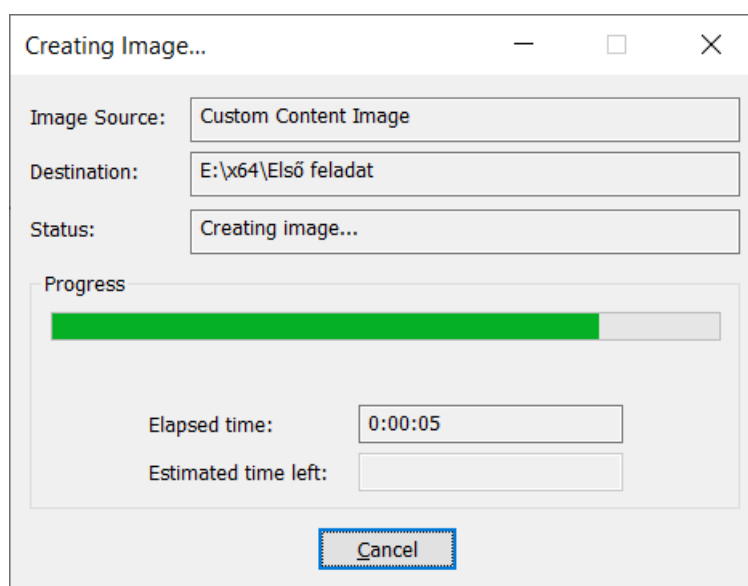
33. kép: Konténerfájl könyvtára
Forrás: a szerző

A kiválasztás után tetszőlegesen elnevezhetjük a létrejövő fájlt, ami nekem „Első feladat” lesz, majd a „Finish” gomb után a „Start” ikonra kattintva megkezdődik a konténerbe helyezési folyamat.



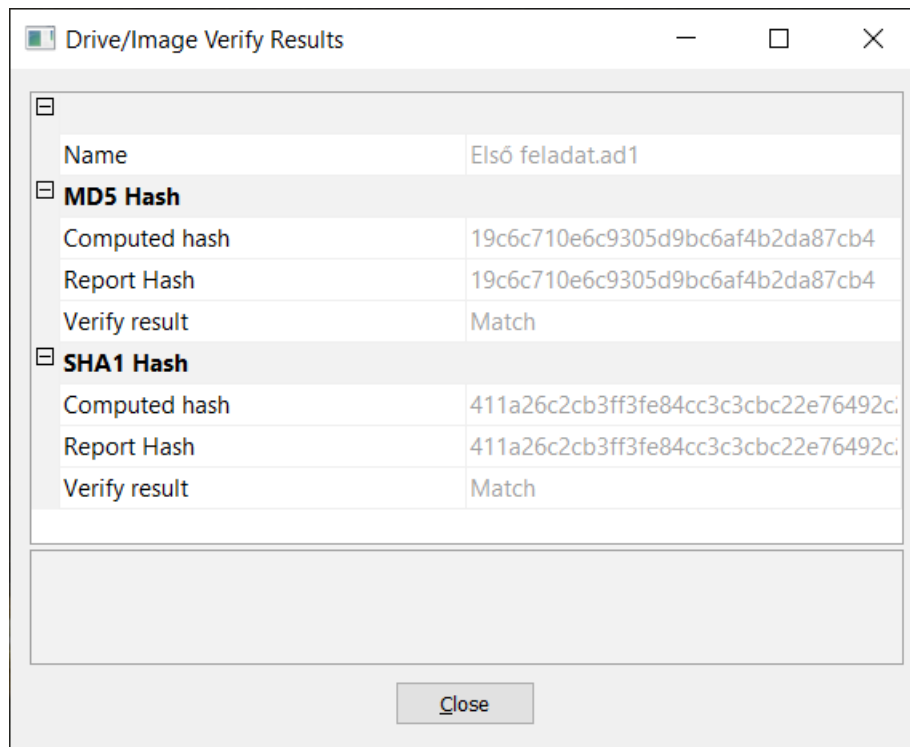
34. kép: Konténerbe helyezés megerősítése
Forrás: a szerző

A konténerbe helyezési folyamat a memórafájl méretétől függően eltarthat egy kis ideig. A valós helyzetben nem csak a memórafájl helyezhető konténerbe, de jelenleg ez elegendő.



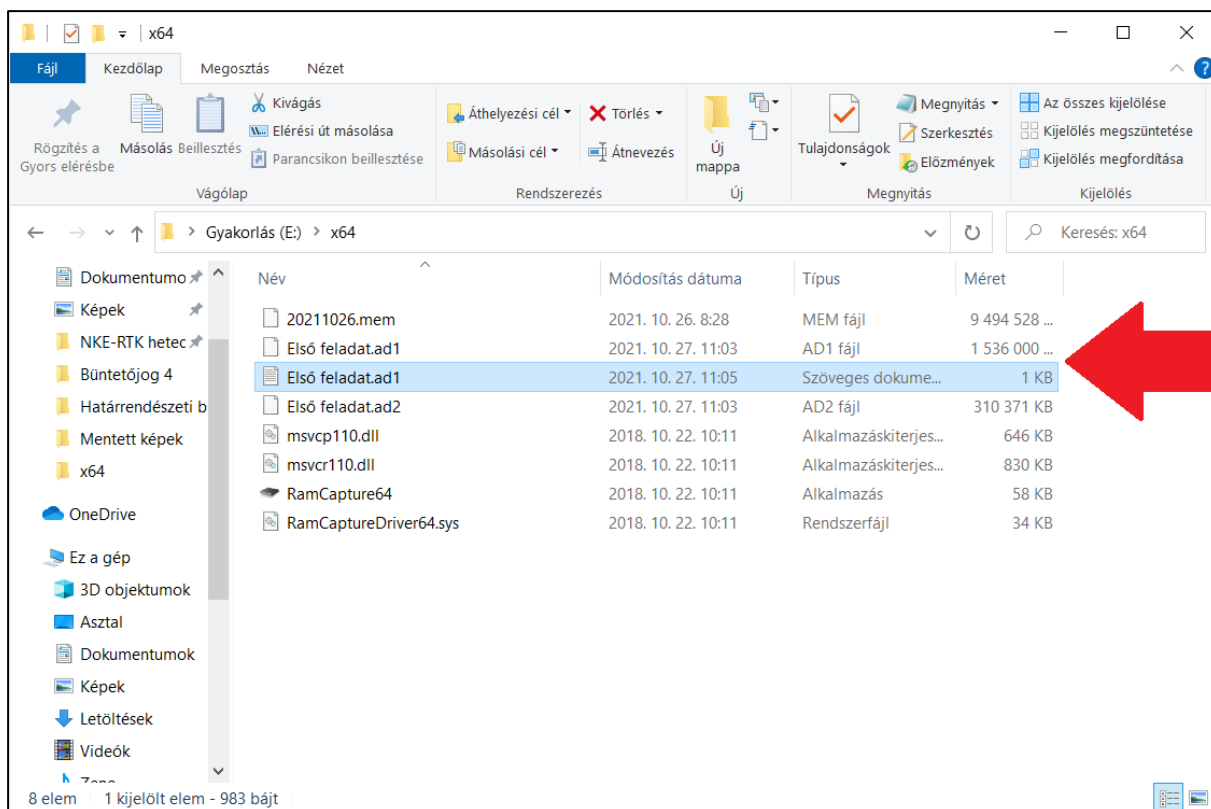
35. kép: Konténerbe helyezési folyamat
Forrás: a szerző

Egy 9 GB-os memóriaképen nálam közel 10 perc alatt hajtotta végre a folyamatot, és 1,5 GB-ra tömörítette a memóriakép méretét. Ezzel elkészült a .AD1 kiterjesztésű állományunk, amely egy hash-kulccsal ellátott konténer, igazolva ezzel az adatok integritását.



36. kép: Konténerfájl hash-kulcsai
Forrás: a szerző

A konténerbe helyezési folyamat eredményét megtekinthetjük a korábban kijelölt cél-mappánkban a fájlkezelőben. A végén egy megerősítési folyamatnak köszönhetően jött létre az AD1 fájl mellé egy AD2, de egyként kezelendők és a hash kulcsuk is megegyező.



37. kép: A konténerfájl könyvtára
Forrás: a szerző

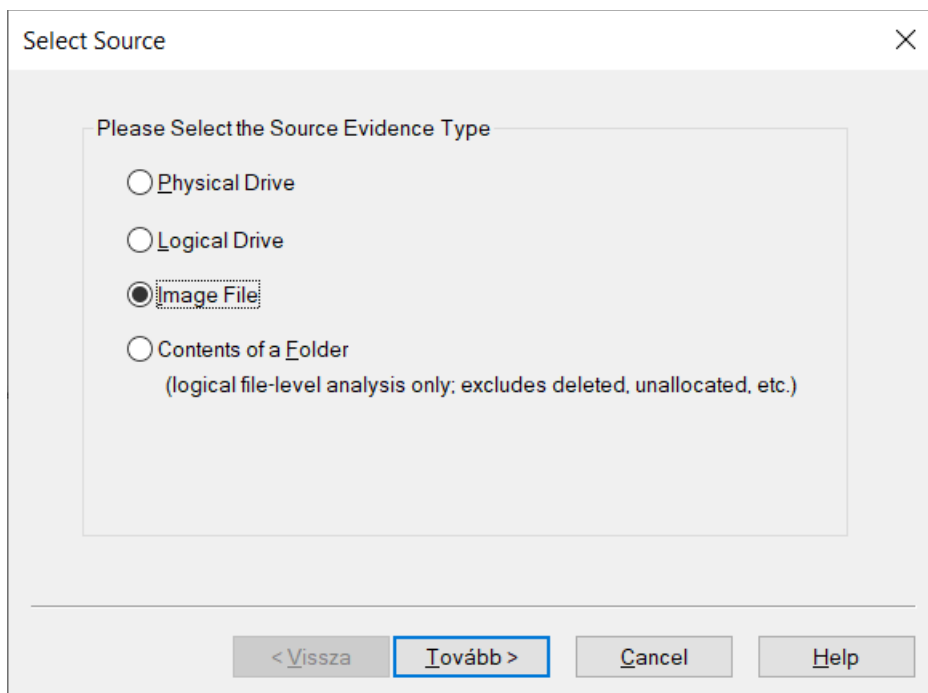
A kisebb méretű szöveges dokumentumban találhatjuk az SHA1 és MD5 hash értékeket. Ebből elegendő, ha az SHA1-et használjuk és rögzítjük valós helyzetben a jegyzőkönyvben, vagy az egyszerűség kedvéért mellékletként lehet csatolni az FTK jelentési dokumentumot a jegyzőkönyvhöz. A pendrive, vagy külső adathordozó biztonságos eltávolítása után a memóriamentési folyamat befejeződött.

4. A RAM ELEMZÉSE

Alapesetben az operatív tár adattartalmának a vizsgálata igazságügyi informatikai szakértői vagy szaktanácsadói kompetencia. Előfordulhatnak azonban olyan esetek is, amikor ezt a vizsgálatot a nyomozó hatóság tagjainak szükséges végrehajtania. Az alábbi fejezetben lényegre törően igyekszem a korábban mentésre került Windows 10 Pro 64 bites operációs rendszernek a memóriaképéből adatokat kinyerni. A Roast Lamb memóriaelemző programmal, képernyőfelvételekkel szemléltetve kerül végrehajtásra a folyamat. Erről részletesebben a tudományos dolgozatomban olvashatunk. A Roast Lamb ZIP fájlt kicsomagolva a Windowsra írt verzióra lesz szükségünk.

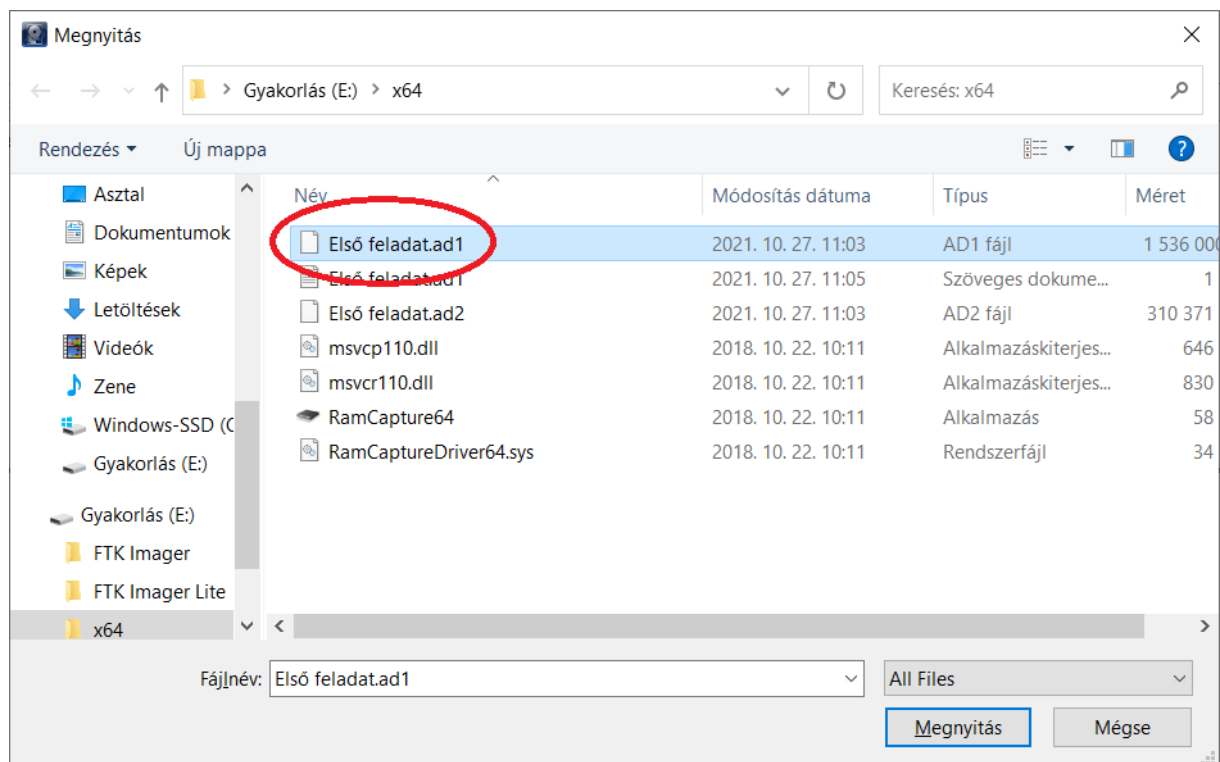
A modellezés éles helyzetben a külső helyszínen mentett RAM adattartalmat konténerbe helyezését, majd jegyzőkönyvi rögzítését követően a nyomozó hatóság objektumában, labor körülmények között kezdődik. Először a konténert, mint egy „ZIP” vagy .rar fájlt ki kell csomagolnunk. Ezt az FTK Imager programmal hajtjuk végre.

Megnyitást követően a „File” fül, „Add Evidence Item”, majd „Image File” opciót választjuk, mert most a memóriakép kicsomagolására kerül sor.



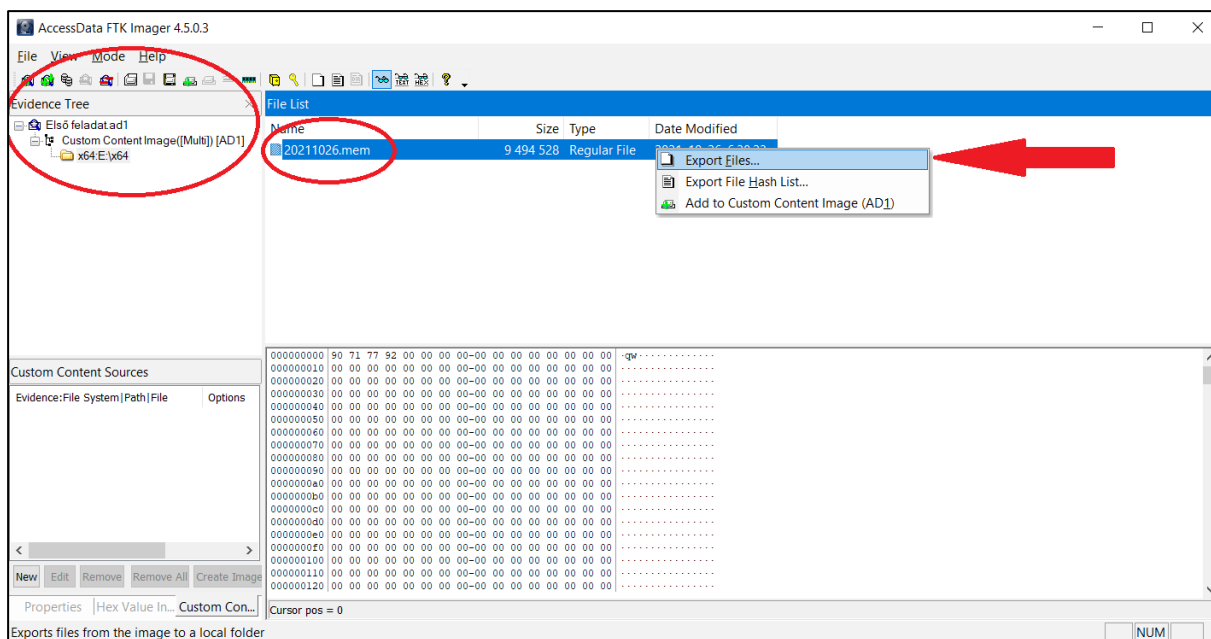
38. kép: Memóriakép kicsomagolása
Forrás: a szerző

A Tovább gombra kattintva kiválasztjuk a mentési könyvtárat, ami nekem továbbra is a pendriveomon található. Itt a .ad1 konténerfájlt kell megnyitni. Majd „Finish”.



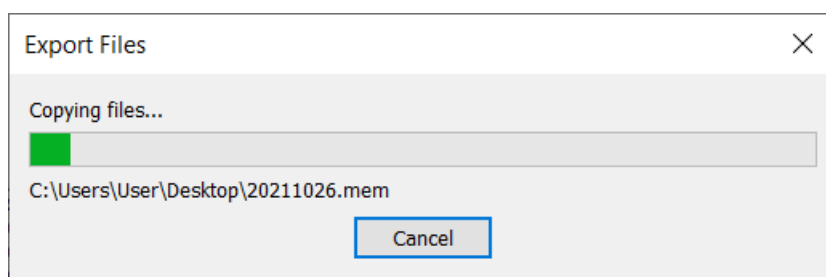
39. kép: Konténerfájl kiválasztása
Forrás: a szerző

A bal oldalon megjelenő „Evidence Tree” mező alatt duplán kattintva addig bontjuk ki a fájlrendszert, amíg megjelenik a memóriaképünk. Ezt követően jobb kattintás a .mem fájlra, majd „Export Files”, és választunk egy tetszőleges helyet a kicsomagoláshoz. Az én esetemben az Asztal lesz.



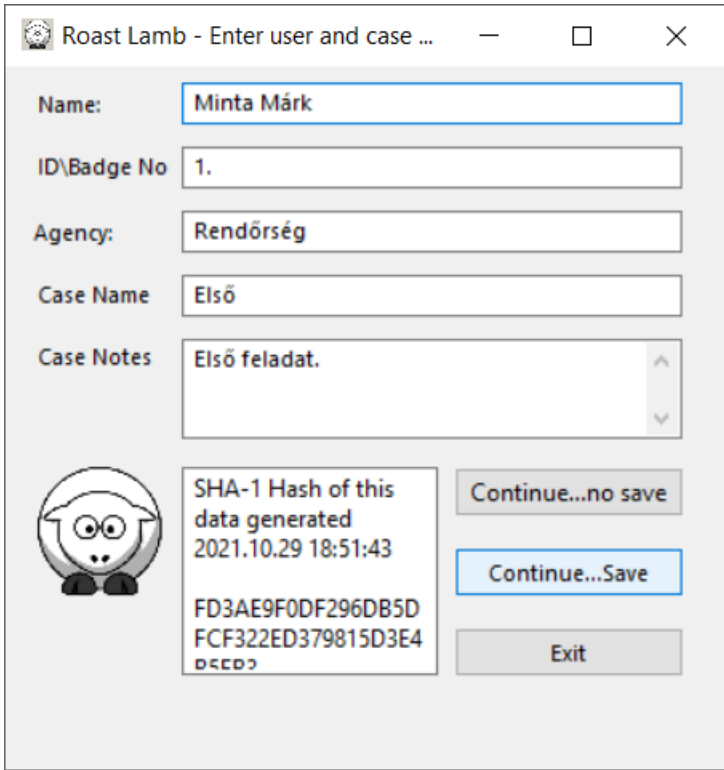
40. kép: Memóriakép kicsomagolása
Forrás: a szerző

A művelet a memóriakép méretétől függően néhány percre eltarthat. Miután sikeresen végrehajtotta a parancsot az FTK Imager, a program bezárható.



41. kép: Memóriakép kicsomagolási folyamat
Forrás: a szerző

Most nyissuk meg a Roast Lamb-et. A felugró ablak mezői tetszőlegesen kitölthetőek. A „Continue...Save” ikonra kattintva kiválaszthatunk a memóriaképpel kapcsolatosan egy mappát, ahova az ügyel kapcsolatos információkat fogja menteni a program egy .txt formátumban. Nekem most is az Asztal lesz a mentési hely, fájlnevének pedig „első elemzés”-t írok.



Roast Lamb - Enter user and case ...

Name: Minta Márk

ID\Badge No: 1.

Agency: Rendőrség

Case Name: Első

Case Notes: Első feladat.

SHA-1 Hash of this data generated 2021.10.29 18:51:43

FD3AE9F0DF296DB5D
FCF322ED379815D3E4
D<EED>

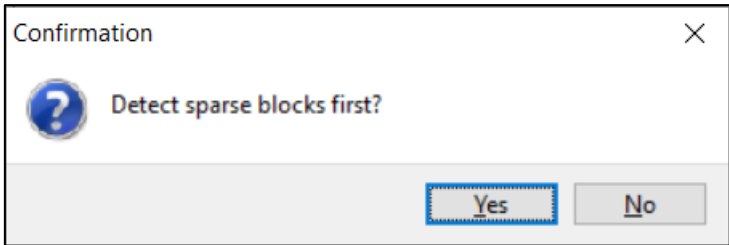
Continue...no save

Continue...Save

Exit

42. kép: Roast Lamb főmenü
Forrás a szerző

Ezután felmerül egy kis ablakban a „Detect sparse blocks first?” kérdés. Ezt a folyamatot most mellőzhetjük.



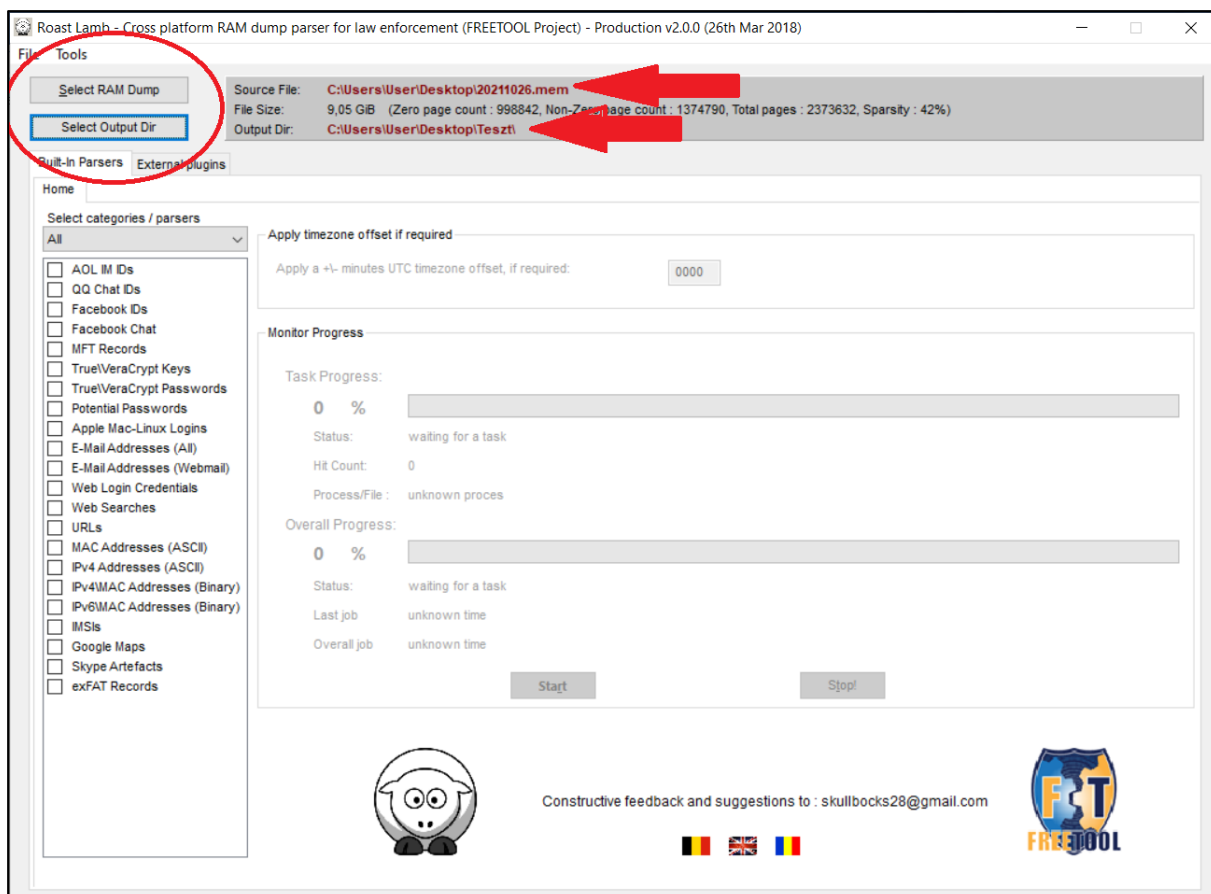
Confirmation

? Detect sparse blocks first?

Yes No

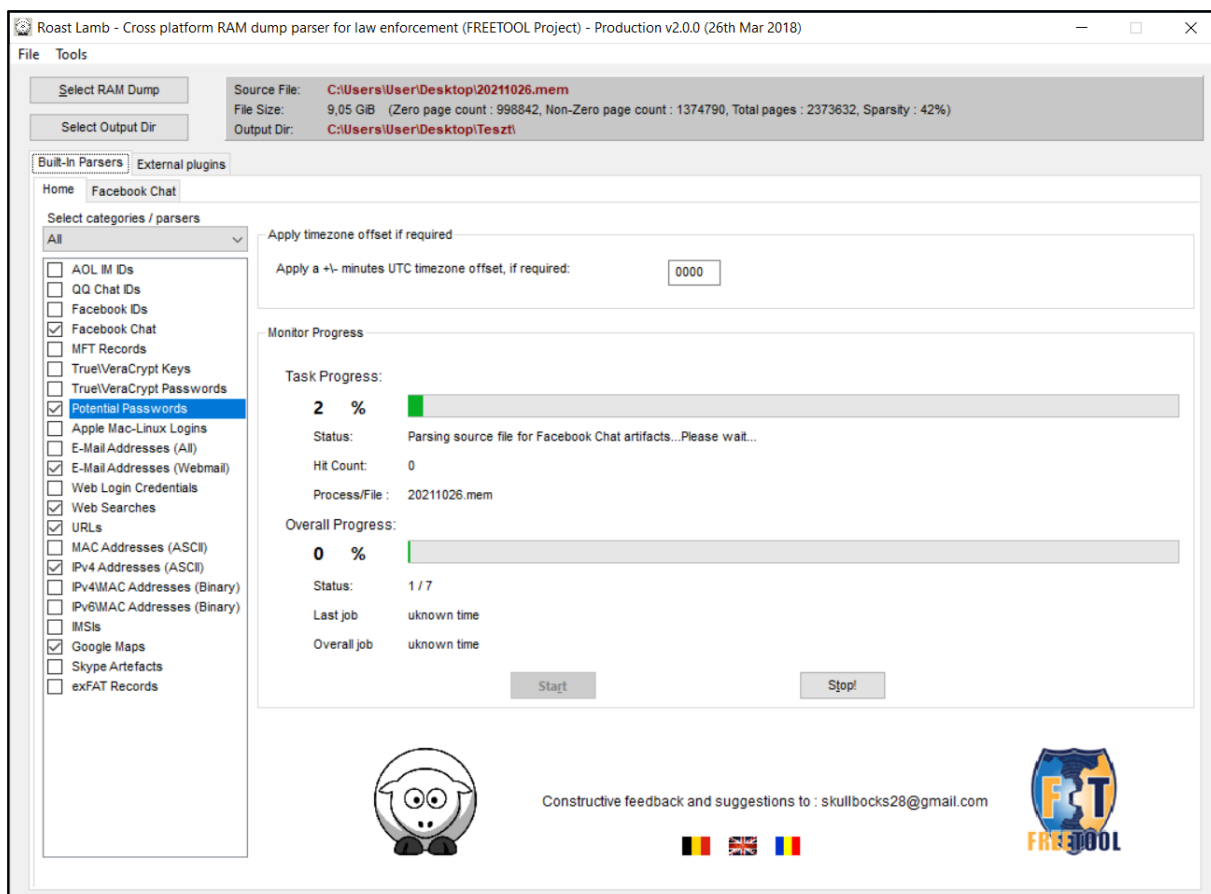
43. kép: Ritka blokkok felmérése
Forrás: a szerző

Megjelenik a Roast Lamb kezelőplatformja. Itt kiválasztjuk a memóriaképet a bal felső sarokban a „Select RAM Dump” füllel, ami nekem az Asztalra lett helyezve, majd a „Detect sparse blocks first?” munkafolyamat most engedélyezhető, amely rövid időn belül véget ér. Az elemzés során létrejövő excel dokumentum mentési helyét a „Select Output Dir” ikonnal módosíthatjuk. Nálam az Asztalon található „Teszt” mappa lesz. Ezt „Yes”-el megerősítjük.



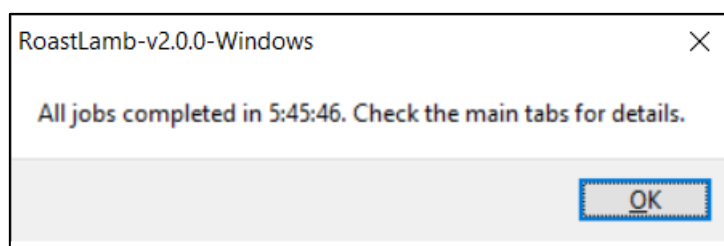
44. kép: Roast Lamb munkafelület
Forrás: a szerző

Ezek után nincs más hátra, mint kijelölni azokat a mezőket, amelyekből álláspontunk szerint a memóriafájlból releváns adatok nyerhetők ki. Amennyiben mind a 22 elemzési folyamatot szeretnénk lefuttatni, a memóriakép méretétől függően akár napokig is elhúzódhat. Nem beszélve arról, hogy egy esetlegesen felmerülő probléma esetén megszakadhat az elemzési folyamat, és kénytelenek leszünk újból elindítani a vizsgálatot, ami rengeteg többlet időt és energiát igényel. Javasolom tehát kategóriákra lebontva (amihez rendelkezésre áll egy külön fül az alkalmazásban) vagy specifikusan néhány folyamatra leredukálva lefuttatni az analízist. Én a képen látható keresési csoportokra voltam kíváncsi, ezért azokra szűkítve a „Start” gombbal indítottam el a műveletet. Kérdés, hogy milyen adatokat nyer ki a program. Megjegyzés, hogy a „Potential Passwords” opció figyelemfelkeltőnek tűnik, mert mégiscsak lehetséges jelszavak fellelhetőségéről van szó, ellenben annak a lefuttatása igényli a leghosszabb időtartamot.



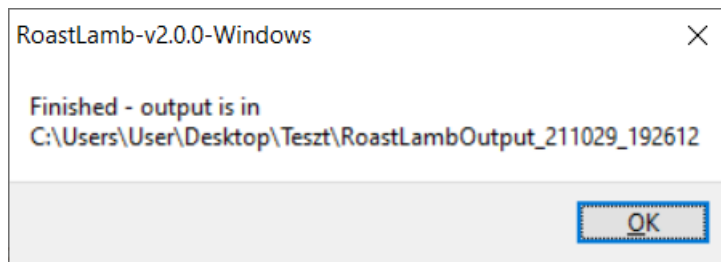
45. kép: Roast Lamb munkafolyamatok
Forrás: a szerző

A vizsgálati folyamat alatt tehát fokozatosan ügyeljünk arra, hogy a programot ne zárjuk be. Nálam 5 óra 45 perc alatt ért véget a vizsgálati folyamat úgy, hogy 6 db keresési kategóriát választottam ki.



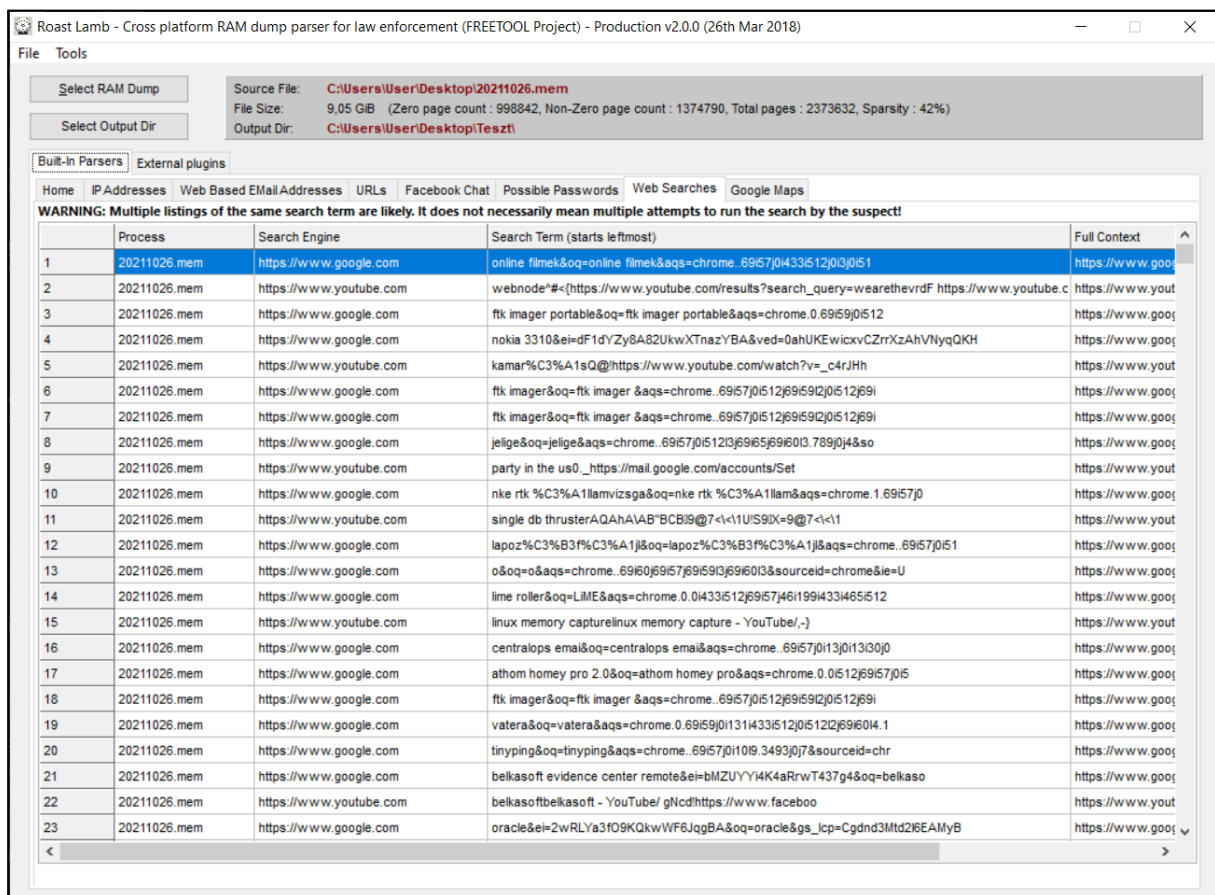
46. kép: Roast lamb munkafolyamat befejezése
Forrás: a szerző

A Roast Lamb egy felugró ablakkal jelzi, hogy a mentési adatok hova lettek rögzítve, ami nálam a korábban említett „Teszt” mappa.



47. kép: Keresési eredmények helye
Forrás: a szerző

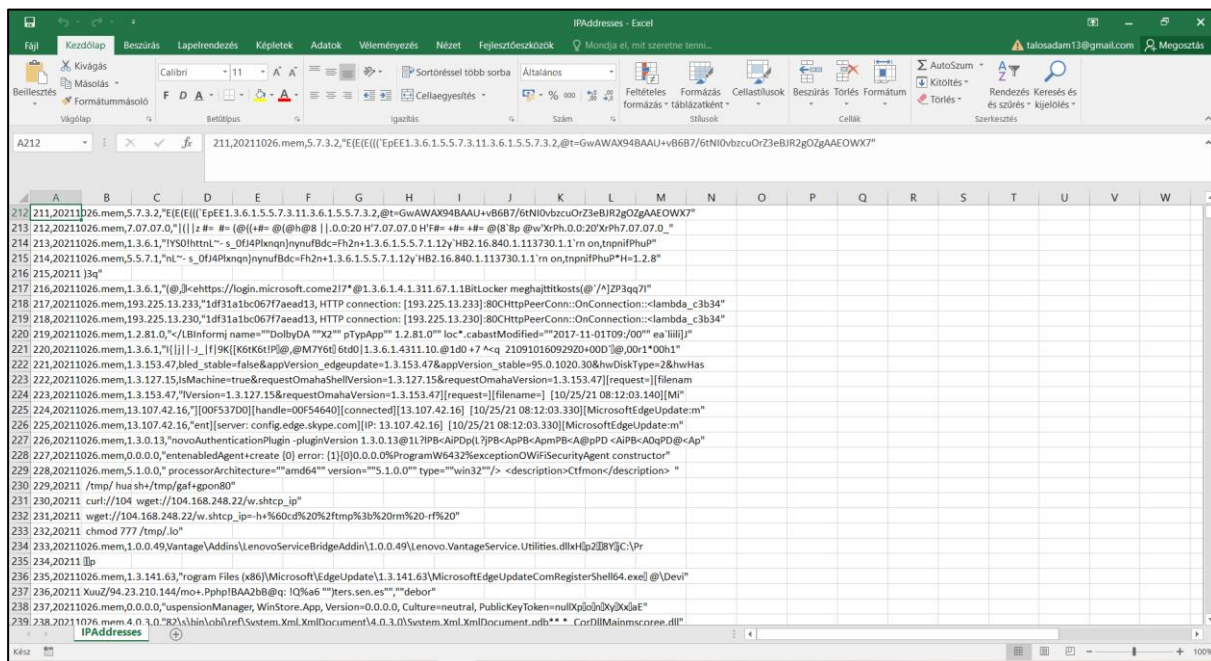
Az vizsgálati eredményeket felhasználóbarát formában a Roast Lamb-ben tekinthetjük meg, illetve annak bezárását követően csak excel dokumentumként, ami figyelem és koncentrációigényes.



48. kép: Vizsgálati eredmények megtekintése
Forrás: a szerző

Ne lepődjünk meg azon, ha egy keresési algoritmusra, pl.: Facebook chatek-re nem ad ki eredményt, hiszen nem minden esetben várható érdemi információ egy-egy művelettől. Ezzel mindig szükséges számolni. A lehetséges jelszavak száma több százezer sorra kiterjedő, óriási méretű táblázatot eredményezett, pedig ez csak egy 9 GB-os memóriakép volt. Gondoljunk

csak bele, mekkora adatmennyiséget szükséges feldolgozni egy 16 vagy 32 GB-os operatív tár esetén.



49. kép: Eredmények Excelben
Forrás: a szerző

Minél nagyobb terjedelmű az Excel dokumentumunk, annál nehezebben fogja a készülékünk betölteni, ezért legyünk erre tekintettel, különösen a „Potential Passwords” kategóriánál. Érdekes és tanulságos lehet, ha valamelyik fontos jelszavunkra rákeresünk az eredmény fájlban az excel kereső parancsával. Amennyiben megtaláljuk valamelyik sorban, akkor az azt jelenti, hogy a gépünk memóriájából készített jelszó-bankkal fel lehet törni a kérdéses jelszavunkkal lezárt fiókunkat. A Google térképekkel kapcsolatos adatokat szélességre és hosszúságra pontosan kiolvashatjuk, illetve a koordinátákat a Google Térképbe begépelve megtekinthetjük, hogy milyen helyhez kapcsolódik. Az elvégzett műveletekről a kimeneti mappában található egy „OutputHashes” szöveges dokumentum, amely hash-azonosítóval látja el a végrehajtott folyamatokat.

5. ÖSSZEGZÉS

A segédlet végéhez érve röviden összegzem az eddig leírtakat, illetve tapasztalataimat. Az eredményes memóriamentés végrehajtása és elemzése felsorolásszinten a következőképpen néz ki:

1. Az adathordozó teljes adattartalmának törlése (Wipe és Formázás)
2. Memóriamentő, telepítést nem igénylő szoftver áthelyezése a külső adathordozóra
3. RAM mentés végrehajtása, majd konténer fájlba helyezése
4. Szakértő vagy szaktanácsadónak a memóriakép elküldése, vagy saját magunk általi elemzés végrehajtása.

Az útmutatóban bemutatott alkalmazásoktól természetesen el lehet térni és az eljárások egyaránt eredményesen lefolytathatók más szoftverekkel. A Belkasoft Live RAM Capturer, a Roast Lamb, illetve az FTK Imager csak az én szubjektív megítélésem alapján a legkézenfekvőbb alkalmazások.