UNIVERSITETI I EVROPËS JUGLINDORE
УНИВЕРЗИТЕТ НА ЈУГОИСТОЧНА ЕВРОПА
SOUTH EAST EUROPEAN UNIVERSITY

Fakulteti **Fakulteti i Shkencave dhe Teknologjive Bashkëkohore**
Programi Studimor **Zhvillimi i softuerit dhe aplikacioneve**

TEZË MAGJISTRATURE

"FORENZIKA DIGJITALE DHE GJURMIMI I *HARD*-DISQEVE"

Kandidate
Dëshira Imeri-Saiti

Mentor
Prof. Dr. Zamir Dika

Janar, 2022

Abstrakti

Forenzika digjitale konsiderohet si një degë relativisht e re në fushën e sigurisë kibernetike që po bëhet gjithnjë e më e rëndësishme me përhapjen e krimeve dhe aktiviteteve të paligjshme në hapësirën kibernetike. Forenzika digjitale është një shkencë e re dhe si e tillë ndjek ndryshimet e shpejta në mjedisin informatik, me një shtrirje në shumë disciplina (si sistemi ligjor, zbatimi i ligjit, menaxhimi i biznesit, teknologjia e informacionit dhe natyra pa limit e internetit), e cila e shndërron atë në një fushë shumë sfiduese që kërkon zhvillim të vazhdueshëm të metodologjive dhe mjeteve për t'iu kundërvënë ndryshimeve gjithnjë e më të reja të krimit kibernetik.

Duke u bazuar në trendin ritës të zhvillimit të teknologjisë dhe ritjen e numrit të krimeve digjitale, në këtë hulumtim fokus i vecantë i është dhënë aspektit statistikor sa i përket krimit kompjuterik si dhe masat për të ulur hovin e krimit kompjuterik, duke përfshirë edhe aspektin etik dhe ligjor në Republikën e Maqedonisë së Veriut (RMV). Në veçanti është shqyrtuar analiza e sfidave të forenzikës digjitale, gjurmimi i *hard*- disqeve, kthimi i fajlave të fshirë nga *hard*- disku, cilësia e tyre pas kthimit, si dhe mundësia për krijim të imazheve forenzike tek *hard*- disqet fizikisht të dëmtuara.

Për të realizuar këtë hulumtim janë përdorur të dhëna statistikore të krimit kompjuterik në RMV prej vitit 2010 deri në vitin 2019 duke u bazuar në të dhëna historike të analizës, krahasimit, korelacionit dhe ANOVA-testit. Hulumtimi vazhdon duke analizuar forenzikën digjitale dhe gjurmimin e katër *hard*-disqeve duke krijuar imazhe digjitale për të njejtit përmes veglave me burim të hapur për krijim dhe analizim të imazheve forenzike FTK *Imager* dhe Autopsy 4.15.0.

Nga hulumtimi konkludohet që numri i *file*-ve të alokuara në një imazh forenzik nuk luan rol në kohëzgjatjen e gjenerimit të raporteve gjatë krijimit të imazheve forenzike përmas FTK *Imager*.

Për dallim të *file*-ve të alokuar, *file*-et e pa analizuara në një imazh forenzik janë në proporcion të drejtë me kohëzgjatjen e gjenerimit të raporteve për imazhet forenzike përmes FTK *Imager.*

Gjithashtu si përfundim vlen të theksohet që FTK *Imager* nuk mund të gjenerojë imazh forenzik kur hard-disku është fizikisht i dëmtuar.

Fjalët kyçe: *hard*-disqet, forenzika digjitale, FTK Imager, Autopsy, Republika e Maqedonisë së Veriut

Abstract

Digital forensics is considered as a relatively new branch in the field of cyber security which is becoming increasingly important with the spread of crimes and illegal activities in cyberspace. Digital forensics is a new science and the fact that this science deals with rapid changes in the information environment, on the other hand affects its scope in many disciplines (such as legal system, law enforcement, business management, information technology and nature without internet limit) which make it a very challenging field that requires continuous development of methodologies and tools to counter the ever-changing changes of cybercrime.

Based on the increasing trend of technology development and the increase in the number of digital crimes in this research, special focus has been given to the statistical aspect in terms of cybercrime as well as measures to reduce the momentum of cybercrime, ethical and legal aspects in R of Northern Macedonia (RMV). In particular, the analysis of the challenges of digital forensics, investigation of hard- drives, recovery of deleted files from the hard disk, their quality after recovery and the possibility of creating forensic images on physically damaged hard drives were examined.

To conduct this research, cybercrime statistical data in the RMV from 2010 to 2019 were used, based on historical data of statistical analysis, comparison, correlation and ANOVA test. The research continues by analyzing digital forensics and investigation of four hard-drives by

creating digital images for the same through open source tools for creating and analyzing forensic images FTK Imager and Autopsy 4.15.0.

From this research it can be concluded that the number of allocated files at a forensic image does not play a role in the duration of report generation when creating forensic images through FTK Imager. Unlike allocated files, unanalyzed files in a forensic image are in direct proportion to the duration of the generation of reports for forensic images through FTK Imager. Also as a conclusion it is worth noting that FTK Imager can't generate forensic image when the hard disk is physically damaged.

Keywords: hard-drives, digital forensic, FTK Imager, Autopsy, Republic of North Macedonia

PËRMBAJTA

1.SFIDAT NË FORENZIKËN DIGJITALE 4
1.1 Analiza e sfidave në forenzikën kompjuterike 4
1.2 Historiku i forenzikës digjitale 5
1.3 Llojet e forenzikës digjitale 7
1.3.1 Forenzika kompjuterike 7
1.3.2 Forenzika celulare 8
1.3.3 Forenzika e rrjetit 8
1.3.4 Forenzika e databazës 10
1.3.5 Forenzika e analizës së të dhënave 11
1.4 Veglat e forenzikës digjitale 11
1.5 Forenzika digjitale e imazheve të diskut 14
1.6 Proceset e forenzikës digjitale 16
1.7 Gjurmimi i *hard*-disqeve 19
1.7.1 *Hard*- disqet dhe karakteristikat 19
1.7.2 Forenzika e *hard* disqeve 21
2. ASPEKTET ETIKE DHE LIGJORE TË FORENZIKËS DIGJITALE NË REPUBLIKËN E MAQEDONISË SË VERIUT 23
2.1 Aspektet etike dhe ligjore në forenzikën kompjuterike 23
2.2 Organizatat e kodeve të etikës të forenzikës digjitale 25
2.3 Analizat statistikore të krimit kompjuterik në Republikën e Maqedonisë së Veriut 27
2.4. Përfundimet 40
3. FORENZIKA DIGJITALE, GJURMIMI I *HARD*-DISQEVE 41
3.1 Ç'ka paraqet imazhi i një disku? 42
3.2 Ekzaminim i provave digjitale 43
3.3 Krijimi i imazheve digjitale te *hard*-diksut 1, 2, 3 dhe 4 përmes FTK Imager 43
3.4 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 1 59

3.5 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 2 66
3.6 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 3 68
3.7 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 4 72
3.8 Montim i imazhit për *hard*-diskun 1 75
3.9 Autopsy 4.15.0 76
3.10 Analiza e imazheve digjitale të krijuara për hard-disqet 1, 2, 3 dhe 4 duke perdorur veglën forenzike digjitale Autopsy 4.15.0 77
3.11 Çka paraqet pamësi i pemës (ang. *Tree Viewer)*? 82
3.12 Përmbledhje e burimit të të dhënave për *hard*-disqet 1, 2, 3 dhe *hard*- diskut 4 88
3.13 Moduli i galerisë së imazheve dhe videove për hard-diskun 1 92
3.14 Vizualizimi i komunikimit në *hard*-diskun 1 94
3.15 Vendndodhja (ang. Geolocation) e fotografive në *hard*-diskun 1, 2, 3 dhe 4 98
3.16 Vija kohore *(ang.Timeline)* e *hard*-diskut 1 100
3.17 Zbulim i *file*-eve (ang. *File Discovery*) 105
3.18 Gjenerim i raportit 107
3.19 Krijimi i imazhit forenzik tek *hard*-disku fizikisht i dëmtuar 110
4. PËRFUNDIME DHE REKOMANDIME 111

LISTA E FIGURAVE

Fig. 1 Tableau eSata Forensic Bridge 44
Fig. 2 Hard-disku 1 46
Fig. 3 Hard-disku 2 47
Fig. 4 Hard-disku 3 48
Fig. 5 Hard-disku 4 49
Fig. 6 Ndërlidhja e hard-diskut me paisjen Tableau 50
Fig. 7 Krijim i imazhit të diskut përmes FTK Imager 4.3.1.1 51
Fig. 8 Përzgjedhja e opcionit disku fizik *(ang.physical drive)* gjate krijimit të imazhit të diskut 52
Fig. 9 Përzgjedhja e hard-diskut për të cilin krijohet imazhi 52
Fig. 10 Destinimi i imazhit që krijohet 53
Fig. 11 Përzgjedhja e llojit të imazhit që do të krijohet 54
Fig. 12 Plotësimi i të dhënave gjatë gjenerimit të imazhit të diskut 55
Figure 13 Pëzgjedhim destinacionin ku dëshirojm të eksportojm imazhin forenzik 56
Fig. 14 Krijimi i imazhit të diskut 57
Fig.15 Verifikim i procesit të krijimit të imazhit të diskut 58
Fig. 16 Rezultati nga verifikimi i imazhit të hard-diskut 1 59
Fig. 17 Artikull i dëshmive FTK-së 63
Fig. 18 Përzgjedhja e diskut fizik gjatë krijimit te imazhit për hard-diskun 1 63
Fig. 19 Shtim i FTK provave duke përzgjedhur diskun fizik 64
Fig. 20 Shtim i evidencës në FTK Imager duke e përzgjedhur burimin 65
Fig. 21 Shtim i evidencës në FTK Imager duke e përzgjedhur diskun fizik 65
Fig. 22 Montim i imazhit (ang. Image mountain) për hard- diskun 1 75
Fig. 23 Analiza e imazhit forenzik të diskut për hard-diskun 1 77
Fig. 24 Analiza e imazhit forenzik të diskut për hard-diskun 1- pjesa II 78
Fig. 25 Analiza e imazhit forenzik të diskut për hard-diskun 1- pjesa III 78
Fig. 26 Analiza e imazhit forenzik të diskut për hard-diskun 2- pjesa I 79
Fig. 27 Analiza e imazhit forenzik të diskut për hard-diskun 2- pjesa II 79
Fig. 28 Analiza e imazhit forenzik të diskut për hard-diskun 3- pjesa I 80
Fig. 29 Analiza e imazhit forenzik të diskut për hard-diskun 3- pjesa II 80
Fig. 30 Analiza e imazhit forenzik të diskut për hard-diskun 4- pjesa I 81
Fig. 31 Analiza e imazhit forenzik të diskut për hard-diskun 4- pjesa II 81
Fig. 32 Katër volumet e hard-diskut 1 83
Fig. 33 Kategorizimi i File Type-it për hard-diskun 1 83

Fig. 34 File-at e fshirë në hard-diskun 1 84
Fig. 35 Tag-im i file-ve të fshirë 84
Fig. 36 File-et e fshira pas tag-imit mund ti gjejm në File Tags 85
Fig. 37 File-et e fshira pas tag-imit te selektuar ne një tag list të krijuar nga ne 85
Fig. 38 Karakteristikat e file-it të fshirë 86
Fig. 39 Rezultatet e Hard- Diskut 1 87
Fig. 40 Përmbledhje e burimit të të dhënave për hard-diskun 1 (ang. Data sources summary of Hard-drive 1) 88
Fig. 41 Përmbledhje e burimit të të dhënave për hard-diskun 2 (ang. Data sources summary of Hard-drive 2) 89
Fig. 42 Përmbledhje e burimit të të dhënave për hard-diskun 3 (ang. Data sources summary of Hard-drive 3) 89
Fig. 43 Përmbledhje e burimit të të dhënave për hard-diskun 4 (ang. Data sources summary of Hard-drive 4) 90
Fig. 44 Gjenerim i rapoteve per hard-disqet 1, 2, 3 dhe 4 krahasuar me përmbledhjen e burimit të të dhënave për hard-disqet 1, 2, 3 dhe 4 91
Fig. 45 Verifikim i raporteve per hard-disqet 1, 2, 3 dhe 4 krahasuar me përmbledhjen e burimit të të dhënave për hard-disqet 1, 2, 3 dhe 4 91
Fig. 46 Galerija e imazheve dhe videove në hard-diskun 1 93
Fig. 47 Galerija e imazheve dhe videove në hard-diskun 2 93
Fig. 48 Galerija e imazheve dhe videove në hard-diskun 3 94
Fig. 49 Galerija e imazheve dhe videove në hard-diskun 4 94
Fig. 50 Vizualizim i komunikimit në hard-diskun 1 95
Fig. 51 Vizualizim i llogaris së përzgjedhur në hard-diskun 1 96
Fig. 52 Snapshot raport për nyje të caktuar në hard-diskun 1 97
Fig. 53 Snapshot raport për nyje të caktuar në hard-diskun 3 97
Fig. 54 Snapshot raport për nyje të caktuar në hard-diskun 4 97
Fig. 55 Pamje nga vendndodhja(ang. geolocation) e fotografisë në hard-diskun 1 98
Fig. 56 Specifikacion i fotografijës nga hard-disku 1 përmes modulit Picture Analyzer Module nga vendndodhja (ang. geolocation) 99
Fig. 57 Specifikacion i fotografive nga hard-disku 3 permes modulit Picture Analyzer Module nga vendndodhja (ang. geolocation) 99
Fig. 58 Specifikacion i fotografijës nga hard-disku 4 permes modulit Picture Analyzer Module nga vendndodhja (ang. geolocation) 100
Fig. 59 Vija kohore (ang.Timeline) e hard-diskun 1 përmes pamjes Counts View 101
Fig. 60 Pamje e vijës kohore të hard-diskut 1 duke përzgjedhur një periudhë kohore të caktuar. 102
Fig. 61 Modaliteti i dytë i pamjes të vijës kohore të hard- diskut 1 përmes pamjes së detajeve (ang. details view) 103
Fig. 62 Modaliteti i tretë i pamjes të vijës kohore të hard- diskut 1 përmes pamjes së listës (ang. list view) 104
Fig. 65 Dritarja komunikuese pas përzgjedhjes së opcionit zbulim i file-eve (ang.File Discovery) 106
Figure 66 Zbulim i file-eve (ang.file discovery) kategorija imazhe te hard diskut 1 107

Fig. 67 Raportet e gjeneruara të vendosura në nyjen Reports 108
Fig. 68 Llojet e raporteve që mund të gjenerohen përmes modulit gjenerim raporti (ang. Generation report) 108
Fig. 69 HTML raport i gjeneruar për hard-diskun 1 109

LISTA E TABELAVE

Tabela nr. 1 Metodat dhe shembujt e perdorimit ne zhvillimin e modelit 10
Tabela nr. 2 Mapa e krimeve kompjuterike 27
Tabela nr. 3 Llojet krimeve kompjuterike në periudhën kohore 2010-2015 32
Tabela nr. 4 Llojet krimeve kompjuterike në periudhën kohore 2016-2019 33
Tabela nr. 5 Numri mesatar i krimeve sipas qyteteve (Sektorët për Punë të Brendshme), 2010-2014 .. 36
Tabela nr. 6 Personat e raportuar sipas gjinisë 36
Tabela nr. 7 Personat e raportuar sipas moshës 38
Tabela nr. 8 Personat e raportuar sipas moshës (%-kumulative) 39

LISTA E GRAFIKONEVE

Grafikoni nr.1 Zinxhiri i proceseve dhe integriteti i provave 17
Grafikoni nr.2 Vepra penale dhe kryerësit ndër vitet 2010-2019 29
Grafikoni nr.3 Veprat penale dhe kryerësit sipas bazës ligjore, vitet 2010-2019 31
Grafikoni nr. 4 Vepra penale sipas qyteteve (Sektorët për Punë të Brendshme) 35
Grafikoni nr.5 Pjesëmarrja e personave të raportuar sipas gjinisë 37
Grafikoni nr. 6 Pjesëmarrja e personave të raportuar sipas moshës 39

HYRJE

Forenzika digjitale është një disiplinë e veçantë e shkencës forenzike dhe në fusha të ndryshme ajo kërkon qasje të ndryshme, vegla të ndryshme, si dhe edukime dhe trajnime të specializuara. Rasti i parë i ndjekur penalisht si krim kompjuterik është evidentuar në vitin 1966.

Forenzika digjitale është degë e shkencave forenzike, lëmi e cila përfshin ruajtjen, identifikimin, nxjerrjen, interpretim, dhe dokumentimin e evidencës digjitale.

Fillet e forenzikës digjitale karakterizohen me kapacitet relativisht të vogël të pajisjeve dhe sasi relativisht të vogla të informacionit. Kjo mundësonte që gjithë *hard*-disku të kopjohej në një tjetër disk. Kopja është përdorur për të analizuar përmbajtjen dhe për tu shfrytëzuar si dëshmi i njëjti material.

Qëllimi përfundimtar është të dish se çfarë është bërë, kur është bërë dhe kush e ka bërë atë. Shprehja "forenzikë digjitale" përdoret si sinonim i forenzikës kompjuterike (e njohur edhe si kibernetikë) por është zgjeruar për të mbuluar hetimin e të gjitha pajisjeve që janë të afta të ruajnë të dhëna digjitale, si pajisjet e rrjetit, telefonat mobil, tabletët, kamerat digjitale, Interneti i pajisjeve (Internet of Things -IoT), pajisjet digjitale në shtëpi dhe media të tjera digjitale të ruajtjes si CD, DVD, USB disqet, SD kartelat, disqet e jashtme dhe back up kasetat (ang. *tapes*).

Forenzika digjitale ka aspekte të ndryshme të zbatimit dhe nuk është e përcaktuar nga një procedurë e veçantë. Ajo merret me analizen e informatave të përfshira brenda kompjuterit dhe të krijuara me sistemet kompjuterike në mënyrë tipike, në interes të parashikimit se çfarë ka ndodhur, kur ajo ndodhi, si ndodhi, dhe kush ishte i përfshirë.

Dëshmitë digjitale mund të jenë të dobishme në rastet penale, kontest civil etj.

Sipas një përkufizimi më të gjerë, forenzika digjitale është gjithashtu përgjegjëse për hetimin e pothuajse të gjitha sulmeve kibernetike kundër sistemeve të kompjuterizuara si *ransomware*,

phishing, sulme me injektim të SQL (*injunction*), sulme të shpërndara të shërbimit (DDoS), shkelje të të dhënave, spiunimi kibernetik (*cyberespionage*), llogari të kompromentuar, qasje të paautorizuar në rrjetet infrastrukturore etj.
Në bazë te burimit të provave digjitale, forenzika digjitale mund të kategorizohet në: Forenzikë kompjuterike, forenzikë të celularëve, forenzikë të rrjetit, forenzikë të bazes së të dhënave etj.

Në këtë hulumtim fokus i vecantë i është dhënë aspektit statistikor sa i përket krimit kompjuterik si dhe masat për të ulur hovin e krimit kompjuterik, aspekti etik dhe ligjor në RMV. Është hulumtuar forenzika digjitale dhe gjurmimi i *hard*- disqeve. Në veçanti është shqyrtuar analiza e sfidave të forenzikës digjitale, gjurmimi i *hard*- disqeve, kthimi i fajlave të fshirë nga *hard*- disku, cilësia e tyre pas kthimit si dhe mundësia për krijim të imazheve forenzike tek *hard*- disqet fizikisht të dëmtuara.

Gjatë kryerjes së hulumtimit janë përdorur disa metoda. Metoda empirike është përdorur gjatë shqyrtimit të të dhënave nga hulumtimet e deri tanishme. Metoda e analizës dhe sintezës është përdorur gjatë analizës së forenzikës digjitale dhe gjurmimit të *hard*- disqeve dhe zbërthimin e tyre në elemente përbërse. Metoda statistikore është përdorur gjatë përpunimit të të dhënave në sferën e krimit kompjuterik duke përdorur krahasimin, korelacionin dhe ANOVA- testet. Metoda e induksionit dhe deduksionit, metoda e induksionit është shfrytëzuar për dhënien e konkluzioneve dhe rekomandimeve ndërsa metoda e deduksionit fillon me studimin e identifikimit të specifikacioneve të forenzikës digjitale dhe veçorive të *hard*- disqeve duke u bazuar në të dhënat gjenerale.

Ky studim është i strukturuar në katër kapituj. Kapitulli i parë përfshinë sfidat në forenzikën digjitale, historiku i forenzikës digjitale, llojet e forenzikës digjitale si dhe gjurmimi i *hard*-disqeve etj. Kapitulli i dytë përfshinë aspektet etike dhe ligjore në RMV, organizatat e kodeve të etikës të forenzikës digjitale si dhe analizat statistikore të krimit kompjuterik në RMV. Në kapitullin e tretë është shqyrtuar forenzika digjitale, krijimi i imazheve forenzike dhe gjurmimi i katër *hard*-disqeve duke shfrytëzuar veglën për krijim të imazheve forenzike FTK Imager si dhe veglën për analizim të imazheve forenzike Autopsy 4.15.0. Në kapitullin e katërt dhe të fundit

janë dhënë konkluzionet nga hulumtimi i kryer dhe rekomandimet e mundëshme në lidhje me forenzikën digjitale, gjurminin e katër *hard*-disqeve si dhe konkluzione dhe rekomandime bazuar në analizën e statistikave të krimit kompjuterik në RMV.

1.SFIDAT NË FORENZIKËN DIGJITALE

1.1 Analiza e sfidave në forenzikën kompjuterike

Forenzika digjitale po shkakton një përplasje masive, në mes dy forcave në dukje të ngurta: sistemit ligjor dhe ate të forenzikës që veprojnë me një ritëm relativisht të ngadaltë dhe të qëllimshëm kundrejt shpejtësisë "verbuese" të teknologjisë (Sammons J. , 2012). Sipas *Internet Live Stats* (2021), ka pothuajse 3.5 miliardë përdorues të internetit në botë që nga gushti 2016, duke mbuluar afro 46.1% të popullsisë së botës. Prandaj, mund të supozohet qartë se kriminalistika kibernetike ka evoluar që kur ka filluar raportimi i incidenteve të krimeve kibernetike, si me mbledhjen e provave nga kompjutorët si edhe me rritjen e qasjes në internet. Megjithëse interneti është një abstrakt universal, ndërkombëtarisht, nuk ka asnjë dokument të vetëm të pranuar njëzëri që siguron praktika standarde dhe as nuk ka një organ drejtues përgjithësisht të pranuar për këtë fushë (Prakash & Duhan, 2020). Sipas, Anstee (2012) shkenca e forenzikës digjitale ka evoluar si një shkencë e lidhur me rikuperimin e provave të vendosura në një sistem kompjuterik, ruajtjen në pajisje nëse këto janë të përhershme ose të fshirjes së dokumenteve elektronike si email-e, imazhe apo sekuencë e pakove të të dhënave të transmetuara përmes një rrjeti kompjuterik. Forenzika digjitale sipas Arnes, (2018) po bëhet gjithnjë e më e rëndësishme me eskalimin e krimit kibernetik dhe krimeve të rënda të lidhura me rrjetin, ku kuptimi i ligjeve dhe rregulloreve që qeverisin komunikimet elektronike, krimet-kompjuterike, dhe ruajtjen e të dhënave kërkon përvetësimin e vazhdueshëm të njohurive, metodave dhe mjeteve të reja. Prandaj është kritike dhe e rëndësishme që studentët e shkencave kompjuterike dhe të sigurisë të marrin pjesë në të kuptuarit themelor të forenzikës digjitale, e patjetërsueshme të marrin pjesë në debate publike dhe të veprojnë si ekspertë në një kontekst ligjor (Arnes, 2018). Sipas, Palmer (2001) forenzika digjitale definohet si: "përdorim i metodave të derivuara shkencërisht dhe të provuara drejt ruajtjes, mbledhjes, vërtetimit, identifikimit, analizës, interpretimit, dokumentimit dhe prezantimit të provave digjitale të nxjerra nga burime digjitale me qëllim të lehtësimit ose çuarjes përpara të rindërtimit të ngjarjeve që konstatohen si kriminale; ose ndihma për të parashikuar veprimet e paautorizuara tregohet se është ndërprerëse për operacionet e planifikuara". Forenzika digjitale është gjithashtu e ndryshme nga rikuperimi i të dhënave, i cili

përfshin marrjen e informacionit që është fshirë gabimisht ose kur për një periudhë kohore ka humbur rryma elektrike ose gjatë ndërprerjes së punës të serverit. Për shembull, në rikuperimin e të dhënave, zakonisht ju e dini se çfarë po kërkoni, ndërsa forenzika digjitale është detyra e rikuperimit të të dhënave që përdoruesit kanë fshehur ose fshirë, me qëllim për të siguruar që të dhënat e rikuperuara të jenë të vlefshme në mënyrë që të mund të përdoren si prova (Nelson, Phillips, & Steuart, 2019). Sfidat e forenzikës digjitale sipas Rogers et. al., (2004) janë: **sfidat teknike** - p.sh. formatet e ndryshme të mediave, kriptimi, steganografia, anti-forenzika, drejtpërdrejt përvetësimi dhe analiza; **sfidat ligjore** - p.sh. çështjet juridiksionale dhe mungesa e legjislacionit të standardizuar ndërkombëtar dhe **sfidat e burimeve** - p.sh. vëllimi i të dhënave, koha e marrë për të përvetësuar dhe analizuar mediat kriminalistike. Henry, Williams, & Wright (2013) kanë kryer në Sans Institute një studim të forenzikës digjitale në veprimtaritë e industrisë private ashtu edhe në ate qeveritare dhe zbulojnë se ekzistojnë pesë fushat e mëposhtme sfiduese: çështjet ligjore të pronësisë dhe privatësisë; mungesa e standardeve dhe mjeteve; mungesa e aftësive, trajnimit, dhe çertifikimi; mungesa e politikës së vendosur; dhe mungesa e ri-shikimit.

Forenzika digjitale përdoret për: hetimet penale, gjyqësinë civile, inteligjencën dhe çështjet administrative (Sammons, 2014). Kryerja e hetimeve të forenzikës kompjuterike kërkon zbatimin e standardeve rigoroze gjatë pyetjeve në gjykatë. Kjo përfshin marrjen e të dhënave (si statike ashtu edhe të paqëndrueshme) në një mënyrë të shëndoshë forenzike, analizimin e të dhënave duke përdorur mjete të forenzikës të pranuara nga gjykata, kërkimin e të dhënave të mbledhura për të gjetur prova dhe në fund paraqitjen e gjetjeve në gjykatë në një raport zyrtar (Hassan, 2019). Sipas, Hassan (2019) nëse këto procedura janë zbatuar gabimisht, ne rrezikojmë të dëmtojmë ose shkatërrojmë provat digjitale, duke i bërë ato të papranueshme në një proces gjyqësor.

1.2 Historiku i forenzikës digjitale

Forenzika digjitale konsiderohet si një degë relativisht e re në fushën e sigurisë kibernetike që po bëhet gjithnjë e më e rëndësishme me përhapjen e krimeve dhe aktiviteteve të paligjshme

në hapësirën kibernetike (Hassan, 2019). Forenzika digjitale është një shkencë e re dhe fakti që kjo shkencë merret me ndryshimet e shpejta në mjedisin informatik, në anën tjetër ndikon shtrirja e saj në shumë disiplina (si sistemi ligjor, zbatimi i ligjit, menaxhimi i biznesit, teknologjia e informacionit dhe natyra pa limit e internetit) e bëjnë atë një fushë shumë sfiduese që kërkon zhvillim të vazhdueshëm të metodologjive dhe mjeteve për t'iu kundërvënë ndryshimeve gjithnjë e më të reja të krimit kibernetik (Hassan, 2019).

Forenzika digjitale si shkencë është më e përhapur 40 vitet e fundit, duke filluar në fund të viteve 1970 si përgjigje ndaj kërkesave për shërbimet nga ana e komunitetit të zbatimit të ligjit (Dezfoli, Dehghantanha, Mahmoud, Sani, & Daryabar, 2013). Rritja e krimeve kompjuterike filloi në 1980-ën kur hetuesit filluan ti shikojnë kompjuterët si burime të provës, e në anën tjetër zbatimi i ligjit filloi përpjekjet fillestare të trajnimit të forenzikës digjitale. Në vitin 1984 Ekipi për Analizë dhe Përgjigje Kompjuterike ofroi ndihmë për zyrat në terren të FBI-së në kërkimiet dhe sekuestrimin e provave kompjuterike si dhe ekzaminimet për mbështetje teknike për hetimet e Byrosë Federale të Hetimit (Prasanthi, 2016). Në vitet 1980, kompjuterët personalë u bënë gjithnjë e më të popullarizuar dhe me rrjedhjen e zhvillimeve të numrit të sistemeve kompjuterike u rrit numri i synimeve për krime të mundshme. Për herë të parë, objektivat përfshinin një gamë të gjerë të infrastrukturës kritike (Glynn, 1984). Sistemi Operativ i Diskut (DOS) ishte i disponueshëm në shumë lloje, përfshirë PC-DOS, QDOS, DR-DOS, IBM-DOS dhe MS-DOS, ndërsa mjetet e forenzikës në atë kohë ishin të thjeshta dhe shumica u gjeneruan nga agjenci qeveritare, të tilla si Policia e Royal Canadian Mounted (RCMP, e cila kishte mjetet e veta hetimore) dhe Shërbimi i të Ardhurave të Brendshme të SHBA-së (IRS), (Nelson, Phillips, & Steuart, 2019).

Sipas, Prasanthi (2016) në vitin 1990 ka filluar përdorimi i internetit dhe ka bërë rritje të konsumimit të teknologjisë që do të thotë se teknologjia është e përfshirë në krime dhe se rritja e shpejtë e internetit lehtësoi sulmet kibernetike. Akademia Ndërkombëtare e Zbatimit të Ligjit është themeluar në vitin 1995 për të zvogëluar krimin, luftuar terrorizmin dhe për të marrë pjesë në njohuri dhe trajnime. Në vitin 1997 u krijua Grupi Punues Shkencor për Provat Digjitale (SWGDE) për të zhvilluar standardet e Forenzikës. Gjithashtu standardet e zhvillimit nga

organet e ndryshme të zbatimit të ligjit janë realizuar gjatë kësaj periudhe dhe ka pak rritje në trajnimin dhe zhvillimin e sektorit privat (Prasanthi, 2016).

Në periudhën e viteve të fundit shkëmbimet elektronike kanë aktivizuar bizneset dhe kanë lehtësuar komunikimin në mënyrë eksponenciale; megjithatë, ata gjithashtu e kanë bërë të njëjtin informacion të ndjeshëm ndaj një morie veprimtarish kriminale, ku aktiviteti që ka lindur për shkak të zhvillimeve në përdorimin e teknologjisë së rrjetit ka shkaktuar dëme miliarda dollarë-she qeverive dhe industrisë private (Zakaras, 2001). Projekt-rezolutat e Kombeve të Bashkuara (2021) për aspektet e ndryshme të sigurisë kibernetike për herë të parë i janë përcjellë Asamblesë së Përgjithshme të Kombeve të Bashkuara nga tre komitetet e saj kryesore (Komiteti i Çarmatimit dhe Siguria Ndërkombëtare; Komiteti Ekonomik dhe Financiar; dhe Komiteti Social, Humanitar dhe Kulturor). Ndoshta zhvillimet më të rëndësishme janë bërë në Komitetin e Çarmatimit dhe Sigurisë Ndërkombëtare, i cili mund të konsiderohet si një forum unik për "lojtarët" kryesorë si SH.B.A., Kina dhe Rusia për të diskutuar ''fundin e lartë'' të kërcënimeve të sigurisë së informacionit sipas (ccdcoe.org, 2021).

1.3 Llojet e forenzikës digjitale

Procesi i hetimeve digjitale të forenzikës, siç rekomandohet nga ekspertët, duhet të kryhet nga persona specialistë, të cilët kanë qasje krejtësisht të paanshme për të siguruar besueshmëri ndaj tyre dhe për të siguruar imazh ndaj organizatave ku do të kryhet hetimi (Horsman, Laing, & Vickers, 2012). Sipas, Hassan (2019) forenzika digjitale është kategorizuar në llojet përkatëse, gjegjësisht në: forenzikën kompjuterike, forenzikën celulare, forenzikën e rrjetit, forenzikën e databazës dhe forenzikën e analizës së të dhënave.

1.3.1 Forenzika kompjuterike

Ky është lloji më i vjetër i forenzikës digjitale; ka të bëjë me hetimin e provave digjitale të gjetura në kompjuterët desktop, në laptopë, në pajisjet e ruajtjes digjitale (si disqet e jashtme të forta dhe kartat SD) dhe në kujtesën e aksesit të rastësishëm (RAM), përveç sistemeve operative dhe gjurmëve të instaluara të aplikacioneve dhe regjistrave të tyre të lidhur (Hassan, 2019). Forensika kompjuterike është thjesht zbatimi i teknikave të hetimit dhe analizës kompjuterike në interes të përcaktimit të provave ligjore. Kryesisht merret me çështjet që kanë

të bëjnë me analizat e mediave kompjuterike ose sistemit kompjuterik për prova digjitale në lidhje me kryerjen e krimit kibernetik, e që gjithashtu mund të përshkruhet si "autopsia e një hard disku kompjuterik" për shkak të mjeteve dhe teknikave të specializuara (Prakash & Duhan, 2020). Sipas, Hassan (2019) aktiviteti kryesor i këtij lloji është rikuperimi i të dhënave të fshira nga hapësira ruajtëse e pajisjes së synuar dhe analizimi i tyre për prova inkriminuese ose shfajësuese.

1.3.2 Forenzika celulare

Forenzika e celularëve është gjithmonë e rëndësishme, por jo shumë njerëz e kuptuan rëndësinë e saj, e që nuk është për t'u habitur. Softueri i forenzikës së telefonave celular nuk mund të funksionojë me shumicën dërrmuese të celularëve, por sot pothuajse çdo laborator i forenzikës kompjuterike ka aftësi kriminalistike të celularëve (Hayes, 2015). Instituti Kombëtar i Standardeve dhe Teknologjis (NIST) në SHBA përcakton forenzikën celulare si “shkenca e rikuperimit të provave digjitale nga një pajisje celulare në kushte të shëndosha forenziko-ligjore duke përdorur metoda të pranuara” (Ayers, Brothers, & Jansen., 2014).

Të dhënat mund të merren nga disa vende të ndryshme në telefona, duke përfshirë memorien e paqëndrueshme, memorien e qëndrueshme dhe kartelat multimediale. Gjithashtu nga përdorimi i *file*-ve rezervë nga *cloud* ose kartelat *SIM* lehtë mund të merren informacione nga këto pajisje, por marrja e një imazhi është më e saktë dhe prodhon të dhëna më të hollësishme (Nelson, Phillips, & Steuart, 2019). Gjithashtu, Nelson et al., (2019) përkufizojn se shumë mjete softuerike janë në dispozicion për leximin e të dhënave të ruajtura në pajisjet mobile. Në mënyrë tipike, këto pajisje lidhen me telefonin pa tel (përmes *Bluetooth* ose *IrDA*) ose me një kabëll dhe gjithashtu lexojnë SIM kartelat duke përdorur një lexues të SIM-kartelave, i cili është një pajisje e kombinuar harduerike & softuerike.

1.3.3 Forenzika e rrjetit

Krimi kibernetik, lufta kibernetike dhe terrorizmi kibernetik janë problemet kryesore që kërcënojnë jo vetëm vendet dhe kompanitë tona, por edhe kompjuterët personalë, ku rrjetet përfaqësojnë një sfidë shumë më të madhe, nga këndvështrimi kriminalistik dhe ato ndryshojnë shumë në madhësi dhe kompleksitet. Me ndihmën e disa mjeteve mund të mbrojmë

infrastrukturën tonë kritike të rrjetit, duke përfshirë “muret e zjarrit” ose (ang. *firewall*) dhe sistemin e zbulimit të ndërhyrjeve (Sammons J. , 2012). Sipas, Ranum (1999) forenzika e rrjetit është “kapja, regjistrimi dhe analizimi i ngjarjeve të rrjetit në mënyrë që të zbulohet burimi i sulmeve të sigurisë ose incidenteve të tjera problematike. Rrjedha e të dhënave përmes rrjeteve mund të kapet si një masë në kohë reale dhe e ruajtur për analiza të mëvonshme ose e analizuar në kohë reale me një mundësi për të ruajtur vetëm segmente të ngjarjeve interesante për analiza të mëtejshme *offline* (ky opsion kërkon më pak hapësirë ruajtjeje) (Hassan, 2019).

Kalimi nga IPv4 në IPv6 kërkonte kohë për t'u kryer dhe për një periudhë kohore këto dy protokolle do të funksionojnë në bashkëpunim, që do të thotë se dobësitë dhe shfrytëzimet e reja të sigurisë do të jenë shfaqur, e cila do të kërkonte analizën e duhur të kriminalistikës (Govil, Kaur, & Kaur, 2008). Subjektet e sigurisë shfaqen kur TCP / IP si një protokoll bartës nga njëra anë dhe në anën tjetër kur teknologjia e informacionit kombinohet me rrjetet SCADA, mund të shkaktohet një dëm i madh në rast të një sulmi të suksesshëm në një rrjet IT-e dhe portat e pajisjeve (Kilpatrick, Gonzalez, Chandia, Papa, & Shenoi, 2008). Sipas, Elavarasi (2016) hetuesit hasin shumë sfida në ngjarje të bazuara në rrjetet në shumë segmente, të tilla fusha janë si: blerja, ruajtja, privatësia, konfiskimi dhe pranueshmëria. Sfidat që hulumtuesit sipas Elavarasi-t (2016) duhet ti kenë parasysh në lidhje me infrastrukturën e rrjetit janë: burimet e të dhënave, granuliteti i të dhënave, integriteti i të dhënave, të dhënat si prova ligjore, çështjet e privatësisë dhe analiza e të dhënave. Ndërsa hetuesit e forenzikës në rrjet po kërkojnë të dhëna të rëndësishme brenda të dhënave të mbledhura, sfidat e tjera që shfaqen në pothuajse çdo analizë të kriminalistikës në rrjetë janë: koha, performancat, kompleksiteti, grumbullimi, ligji, fshehja e shkeljes dhe sistemet e rrjetit.

Sipas Pichan, lazarescu & Soh (2015) hetimet i grupuan në tre grupe, gjegjësisht në: forenzikën ndaj klientit, “*cloud*” forenzikën dhe forenzika e rrjetit. Sipas rezultateve të hulumtimeve forenzika në “*cloud*” nuk është forenzikë e rrjetit të internetit ose forenzikë klasike kompjuterike, por një brend krejtësisht i rri për më tepër është një përzierje e teknikave tradicionale kriminalistike dhe aplikacioneve të tyre në një mjedis të rri si “*cloud computing*” (Du, 2020). Informatika në “*cloud*” ka potencial të bëhet një nga zhvillimet më transformuese

në historinë e informatikës, duke ndjekur gjurmët e kornizave kryesore, minikompjuterëve, *PC*-ve (kompjutera personalë) dhe telefonave inteligjentë (Perry, Hatcher, Mahowald, & Hendrick, 2009).

1.3.4 Forenzika e databazës

Forenzika e databazës investigative është një degë e forenzikës digjitale që shqyrton përmbajtjen e bazës së të dhënave për të identifikuar, zbuluar, përvetësuar, analizuar dhe rindërtuar incidentet e bazës së të dhënave, si dhe për të ndërtuar një afat kohor kronologjik të aktiviteteve të ndërhyrjes (Olivier, 2009). Në vitin 2008, nga ana e (Fowler, 2008) u propozua një analizë kriminalistike të serverit SQL, ku metodologjia për të mbledhur dhe analizuar provat nga MSSQL bazat e të dhënave të serverit përbënte katër faza si: hetim-përgatitja, verifikimi i incidentit, mbledhja e objekteve dhe analiza e artefakteve. Sipas studimit të (Ogutu, 2016) qasja e hetimit forenzik për të testuar pasurinë kriminalistike të "*storage engines*" në gjenerimin e qëndrueshëm të të dhënave kriminalistike në sistemet MySQL DBMS, përmbante tre procese të hetimit si: analiza paraprake, ekzekutimi, dhe analiza.

Metoda	**Shembuj**
Baza e të dhënave, modelet e procesit të hetimit kriminalistik	MySQL identifikimi, objekte koleksioni, analizë artefaktesh dhe raportet
Databaza e algoritmeve të hetimit kriminalistik	monokromatik, RGB, RGBY, a3D, Bitmap
Baza e të dhënave artefaktet e hetimit kriminalistik	Memorie, të dhëna, vlerat e regjistrit, regjistri i vlerave, regjistrime ngjarjesh etj.
Baza e të dhënave mjetet e hetimit kriminalistik	Log Miner- Oracle
	Gjurmë SQL & SQL Profiler - MS SQL Server
	ProfilerEventHandler - My SQL
Databaza e metodave të hetimit kriminalistik	Politikat, autorizimi, burimet e vërtetimit, OS, Baza e të dhënave, burimet e rrjetit etj.
Databaza e metodave të zbulimit kriminalistik	Zbulimi i krimit, lloji i bazës së të dhënave, lloji i sulmit, koha dhe burimet e sulmit etj.
Databaza e metodave të mbledhjes kriminalistike	**Blerja e drejtpërdrejtë (ang. Live acquisition**)-mbledhja e të dhënave nga artefakte të paqëndrueshme si memoria e SQL, memoria e të dhënave etj.
	Blerja e vdekur (ang. Dead acquisition)-mbledhja e të dhënave nga artefakte jo të paqëndrueshme si regjistrat e transaksioneve, të dhënat etj.
	Blerja hibride (ang. Hybrid acquisition) -Kombinimi i të gjallëve dhe të vdekurve, për të mbledhur të dhëna më të mira të mundshme.
Metodat e ruajtjes kriminalistike të bazës së të dhënave	Funksionet Hash
Metodat e analizës kriminalistike të bazës së të dhënave	Rindërtimi dhe rikuperimi i aktiviteteve të bazës së të dhënave.

Tabela nr. 1 Metodat dhe shembujt e përdorimit në zhvillimin e modelit

Burimi: Chopade, Rupali & Pachghare, V.K. (2019). Digital Investigation: Ten years of critical review on database forensics research. (29), Elsevier, 180-197

Sipas, Chopade & Pachghare (2019) menaxhimi i bazës së të dhënave dhe njohuritë e hetimit kriminalistik bazuar në hetimin konceptual që është paraqitur nga Razak, Othman, Aldolah &

Ngadi (2016) përbën modelin e zhvilluar duke mbajtur fokusin në algoritmet e hetimit, në artefaktet, mjetet si "*log-miner*" dhe "*SQL Profiler*". Janë përdorur metoda të ndryshme të hetimit kriminalistik dhe janë marrë gjithashtu në konsideratë si hetimi, mbledhja, analiza, zbulimi dhe ruajtja. Gjitahshtu janë dhënë disa shembuj të secilës metodë në tabelë nr.1 ku për të zhvilluar këtë model, ata kanë shqyrtuar katërmbëdhjetë modele të procesit të hetimit të forenzikës digjitale.

1.3.5 Forenzika e analizës së të dhënave

Teknologjia e Internetit me rritjen e shpejtë mund të shkaktojë krime kibernetike të kryera nga sulmuesit, ku lloje të ndryshme të pajisjeve digjitale po përdoren për të kryer një sulm. Për të zbuluar një veprimtari të tillë kriminale, hetuesi kriminalistik duhet të përdorë metoda të ndryshme të rikuperimit të të dhënave dhe një kornizë praktike (Salunkhe, Bharne, & Padiya, 2016). Ekzistojnë lloje të ndryshme të mjeteve forenzike sipas Salunkhe et.al., (2016), gjegjësisht (FTK), softuere falas, teknika dhe mjete që janë në dispozicion për hetimin e kriminalistikës së *file*-ve si "Pema e Vendimit" (DT) për gjenerimin, ruajtjen dhe analizën e të dhënave të marra nga *file*-et e regjistrave të cilat paraqiten si prova në analizën kriminalistike të *file*-ve. Ekzistojnë lloje të ndryshme të aplikacioneve të forenzikës së analizave të të dhënave sipas Hassan (2019), gjegjësishtë forenzikë për aplikacionet specifike (p.sh., kriminalistikë në shfletuesin e uebit), kriminalistikë e sistemit të *file*-ve (NTFS, FAT, EXT), kriminalistikë e pajisjes harduerike, kriminalistikë multimediale (teksti, audio, video dhe imazhe-ve) dhe kriminalistikë e kujtesës [RAM (memorje e paqëndrueshme)].

1.4 Veglat e forenzikës digjitale

Meqenëse shumë lloje të provave digjitale mund të jenë të paqëndrueshme dhe të manipulohen lehtësisht, ruajtja e besueshme e provave përmes përdorimit të mjeteve dhe metodave të standardizuara kriminalistike është bërë thelbësore (Arnes, 2018). Sidoqoftë, veglat e fornzikës digjitale lejojnë që të rikuperohen *file*-et ose fragmente të *file*-eve të fshira që mund të ndihmojnë në rindërtimin e ngjarjeve kryesore të një rasti, ku *file*-et e fshira mund të rikuperohen lehtësisht duke kontrolluar emrat e *file*-ve të fshirë që mbahen në drejtoritë e *file*-ve, por nuk është e pazakontë që emrat e *file-ve* të fshira të ripërdoren para se të bëhet ndonjë

ndryshim në "*metadata*-at" (Boddington, 2016). Aftësia për të përdorur teknikat e duhura digjitale kriminalistike dhe mjetet ndryshojnë sipas agjencive dhe vendndodhjeve gjeografike, ku këto teknika dhe mjete nuk janë të mjaftueshme për të ecur në hap me ndryshimet në pajisjet digjitale (Kao, Wu, & Tsai, 2020). Diapazoni i forenzikës digjitale përfshin pajisje kompjuterike, servera rrjeti dhe aparate celulare. Sipas Kao, Wu, & Tsai (2020) më poshtë janë përshkruar veglat digjitale të forenzikës kriminalistike:

a) **Forenzika e Memories**: Paqëndrueshmëria (ang. *Volatility*), *WindowsSCOPE, RAM Capturer*, *Magnet RAM Capture*, dhe *Memoryze*.

b) **Forenzika e Pajisjeve Mobile**: *CelleBrite* UFED, XRY, dhe *Oxygen Forensic Suite*.

c) **Forenzkia e Rrjetit**: *Wireshark*, *Network Miner*, *Xplico*, dhe *E-Detective*.

d) **Forenzika Kompjuterike**: *EnCASE, FTK, Sleuth Kit Autopsy, TCT, dhe DEFT*.

NIST (Instituti Kombëtar i Standardeve dhe Teknologjisë) ka nisur Projektin e Testimit të Veglave të Forenzikës Kompjuterike (CFTT), i cili përcakton një "metodologji për testimin e veglave të softuerit të forenzikës kompjuterike përmes zhvillimit të procedurave të testimit të specifikimeve të mjeteve të përgjithshme, kritereve të provës, grupeve të provave dhe pajisjeve të provës" (Sammons J. , 2012). Sipas B.V. Prasanthi (2016) fusha e forenzikës digjitale është bërë e njohur gjatë viteve të fundit, me përdorimin në rritje të të dhënave digjitale dhe telefonave celularë. Forenzika digjitale është bërë më e spikatur, madje edhe krimet kompjuterike po rriten në hap me kohën, sepse kjo fushë do të mundësojë gjetjen e provave thelbësore elektronike, nëse ato ishin humbur, fshirë, dëmtuar, apo të fshehura dhe të përdorura për të ndjekur penalisht personat që besojnë se e kanë sulmuar me sukses sistemin. Sipas Prasanthi (2016) nga veglat që janë falas të kriminalistikës kompjuterike, gjegjësishtë për veglat e diskut dhe kapjen e të dhënave përdoren veglat përkatëse: *Arsenal Image Mounter*; *DumpIt*; Imazhi Kriminalistik *EnCase*; Detektor i Diskut të Enkriptuar; *EWF MetaEditor*; Formati *FAT32*; Përvetësimi i Forenzikës së Uebfaqeve; Imazhe *FTK*; *Guymager*; *Live RAM Capturer*; *NetworkMiner*; *Nmap; Magnet RAM Capture; OSFClone; OSFMount; Wireshark; Disk2vhd*.

Autopsia sipas *sleuthkit.org* (2021) është një program i thjeshtë për t'u përdorur, i bazuar në *GUI* (ndërfaqja grafike e përdoruesit), i cili ju lejon të analizoni me efikasitet *hard*- disqet dhe celularët inteligjentë. Ka një arkitekturë *plug*-in që ju lejon të gjeni module shtesë ose të zhvilloni module të personalizuara në Java ose Python. Ndërsa, The Sleuth Kit (2021) është një koleksion i veglave të linjës komanduese dhe një biblioteke *C* që ju lejon të analizoni imazhet e diskut dhe të rigjeni *file*-et prej tyre, e që gjithashtu është përdorur në prapaskenë të Autopsi-së. Analizimi i të dhënave në Autopsi përdor rrjedhën e mëposhtme të punës sipas sleuthkit.org (2021):

Krijimi i një rasti (ang. *Create a Case*): për të krijuar një rast, përdoret opsioni "Krijo një rast të ri" në ekranin e Mirëseardhjes ose nga menyja *File*. Në këtë mënyrë do të fillojë krijimi i një rasti të ri dhe ku do të duhet të emërohet me emrin e rastit në një direktorium për të ruajtur rezultatet e rastit në të, në të cilën mund të sigurohen numri i rasteve dhe emrat e vlerësuesve.

Shtimi i burimit të të dhënave: një ose më shumë burime të të dhënave i shtohen rastit. Burimet e të dhënave përfshijnë imazhe të diskut dhe *file* lokale. Do t'ju kërkohet të specifikoni burimin e të dhënave për të shtuar, ku Autopsia do të kryejë një ekzaminim themelor të burimit të të dhënave dhe mbush një bazë të dhënash me një hyrje për secilin *file* në burimin e të dhënave. Asnjë përmbajtje nuk analizohet gjatë procesit, vetëm *file*-et renditen dhe në vazhdim do t'ju kërkohet një listë e moduleve të marrjes (*ingest modules*) për t'u aktivizuar (sleuthkit.org, 2021). Pasi të konfiguroni modulet e marrjes, mund të duhet të prisni që Autopsia të përfundojë ekzaminimin bazë të burimit të të dhënave dhe ekzaminimin themelor të burimit të të dhënave, e pastaj modulet e marrjes do të fillojnë të analizojnë përmbajtjen e *file*-it.

Analizoni me modulet *ingest* (ang. *Ingest Modules*)): pasi të jetë shtuar burimi i të dhënave, modulet *ingest* funksionojnë në sfond për të analizuar të dhënat, ku rezultatet janë postuar në ndërfaqe në kohë reale dhe japin alarme sipas nevojës. Shembujt e *ingest module*-ve përfshijnë llogaritjen dhe kërkimin e *hash*-it (*hash calculation and lookup*), kërkimin e fjalëve kyçe (*keyword searching*), dhe nxjerrjen e objekteve në internet (*web artifact extraction*). *Ingest* modulet analizojnë *file*-et në një renditje progresive në mënyrë që *file*-et në direktoriumin e një

përdoruesi të analizohen para *file*-ve në dosjet e tjera sipas sleuthkit.org (2021), Modulet standarde të përfshira në Autopsi janë: moduli i kërkimit të bazës së të dhënave *Hash*, moduli i identifikimit të llojit të *file*-ve, moduli i ekstraktimit të *file*-ve të zhvendosur, moduli *EXIF Parser*, moduli i kërkimit të fjalëve kyçe, email modul *Parser*, moduli i zbuluesit të mospërputhjes së zgjatjes, moduli verifikues *E01*, moduli i analizuesit Android, moduli për identifikimin e *file*-eve dhe moduli *PhotoRec*.

Analiza manuale: përdoruesi shfleton në ndërfaqet, përmbajtjet e *file*-ve dhe rezultateve të modulit për të identifikuar provat, ku artikujt më interesantë mund të etiketohen për raportim dhe analizë të mëvonshme.

Gjenerimi i raportit: përdoruesi fillon një raport përfundimtar bazuar në etiketat ose rezultatet e zgjedhura.

1.5 Forenzika digjitale e imazheve të diskut

Në studimin e Breitinger & Baggili (2017) janë analizuar gjithsej 715 artikuj të sigurisë kibernetike nga vitet 2010 deri më 2015, nga konferenca dhe revista në lidhje me përdorimin e të dhënave. Së pari Breitinger & Baggili kanë kategorizuar origjinën e të dhënave (d.m.th., e krijuar nga kompjuteri, e krijuar nga eksperimenti ose bota reale), pastaj kanë analizuar disponueshmërinë e saj dhe së fundmi, llojet e ndryshme të të dhënave (p.sh., *maleware*, imazhe të diskut, etj.), ku rezultatet tregojnë se shumica e grupeve të të dhënave janë gjeneruar me eksperimente (56.4%) të ndjekur nga të dhënat e botës reale (36.7%) dhe nga ana tjetër, 54.4% e artikujve përdorin të dhënat ekzistuese. Korporata e të Dhënave Reale, *Digital Corpora* (2019) ose (RDC) është një koleksioner i të dhënave të para të nxjerra nga pajisjet që mbajnë të dhëna që blehen në tregun sekondar në të gjithë botën, ku shumë studime kanë treguar që *hard* disqet, telefonat celularë, memoriet USB dhe pajisjet e tjera që mbajnë të dhëna hidhen shpesh nga përdoruesit e tyre origjinal pa u pastruar të dhënat më parë dhe me blerjen e këtyre pajisjeve dhe nxjerrjen e të dhënave të tyre *Corpora* ka krijuar një grup të dhënash që imiton nga afër të dhënat siç gjenden në botën reale. Që nga 21 Shkurt 2011, sipas të dhënave nga digitalcorpora.org (2021) nxjerrja e të dhënave nga pajisjet përbëhet nga: 1,289 imazhe të *hard* disqeve që variojnë në madhësi nga 500 MB deri në 80 GB; 643 imazhe të

memorieve *flash* (USB, *Sony Memory Stick*, SD dhe të tjera), që variojnë nga 128 MB deri në 4 GB; 98 CDROM dhe një total prej 70 TB të të dhënave (të pakompresuara).

Sipas Moch & Freiling (2009) ka disa mënyra për të marrë imazhe interesante nga *hard* disku për trajnimin e hetuesve digjitalë, ku mënyra e parë dhe më e dukshme është ndërtimi i tyre ose qasja manuale dhe në këtë rast, një instruktor përgatit me kujdes një imazh të *floppy* disk-ut ose *hard* disk-ut me *file* të veçantë dhe prova artificiale, ndërsa imazhi që rezulton u shpërndahet më pas studentëve në internet ose në një USB. Qasja e dytë përfshin një formë të veçantë të rasteve "reale", domethënë ato të prodhuara duke përdorur *honeypots*, ndërsa shkurtimisht, një *honeypots* është një kompjuter që është i lidhur në rrjet në mënyrë që të mund të sulmohet dhe kompromethohet sipas Moch & Freiling bazuar në Provos & Holz (2007), e cila është e pajisur me softuer special të monitorimit "të ngjashëm me *rootkit*" që mundëson një analizë të hollësishme në rast të post-incidentit, d.m.th., e vërteta themelore e një incidenti dihet kryesisht dhe *honeypots* nuk kanë kufizime reale të privatësisë sepse ato rezultojnë nga aktivitete të paligjshme të sulmuesve dhe sistemi origjinal është artificial. Qasja e tretë sipas Moch & Freiling quhet qasja e dorës së dytë, i cili konsiston në përvetësimin e një sasie të madhe të *hard* disqeve të dorës së dytë dhe dhënien e këtyre studentëve për analiza. Kjo qasje është gjithashtu e përshtatshme për të rritur ndërgjegjësimin me studentët për vlerën e të dhënave të tyre personale, meqenëse provat e gjetura janë në një farë kuptimi "reale" dhe kjo qasje ka një faktor të lartë motivimi.

Hapi i parë në gjenerimin sintetik të të dhënave është përcaktimi i rasteve të përdorimit të të dhënave, për shembull, në një klasë digjitale të forenzikës, ku studentët do të testohen në njohuritë e tyre në lidhje me analizën e *hard* diskut, do të duhet të kërkojnë në imazhet e diskut për gjurmë të *malware*-ve ose të rikuperojnë fragmente të të dhënave multimediale duke përdorur mjetet përkatëse (Yannikos, Graner, Steinebach, & Winter, 2014). Imazhet e diskut mund të krijohen në një kohë të arsyeshme manualisht ose përmes skriptimit. Gjithashtu, sipas Yannikos et. al., nëse detyrave të ndryshme u caktohen studentë të ndryshëm (p.sh., një student duhet të rikuperojë *file*-t JPEG dhe një student tjetër duhet të kërkojë gjurmët e një *rootkit*-i), variacionet më të rëndësishme do të duhej të përfshiheshin në imazhet e diskut. Hapi

i dytë në procesin e gjenerimit është specifikimi i një skenari të botës reale. Shembull i tillë është një kompjuter që përdoret nga shumë individë, të cilët zakonisht instalojnë dhe heqin softuere, shkarkojnë, kopjojnë, fshijnë dhe i mbishkruajnë *file*-t, ndërsa hapi i tretë është krijimi i një modeli që të përputhet *file*-i dhe të shërbejë si bazë e një simulimi, i cili është edhe hapi i fundit (Yannikos, Graner, Steinebach, & Winter, 2014).

1.6 Proceset e forenzikës digjitale

Proces i forenzikës digjitale është një metodë normative e cila kryen hetime të forenzikës digjitale dhe kryesisht është i bazuar në një proces hetimor tradicional të forenzikës fizike i cili përfshin të gjitha fazat e kërkuara (Arnes, 2018). Këto faza sipas Arnes, përfshijnë notifikimet origjinale, përmes raportimit të prezantimit përfundimtar të gjetjeve dhe që gjithashtu është e rëndësishme, sepse nga hetimet mund të verifikohet ndikimi i një incidenti, për të ditur nëse ka pasur shkelje serioze, si p.sh. humbja e të dhënave konfidenciale etj. Shkenca e forenzikës digjitale është akoma në fillimet e saj dhe një fushë e njohur për kërkime që kërkon një metodologji standarde për ta bërë procesin e forenzikës digjitale më të saktë dhe efikase, ku modeli i parë i propozuar përmbante katër hapa: blerjen (ang. *acquisition*), identifikimin, vlerësimin dhe pranimin, ndërsa që atëherë, modele të shumta procesi janë propozuar për të shpjeguar hapat e identifikimit, blerjes, analizimit, ruajtjes dhe raportimit mbi provat e marra nga pajisje të ndryshme digjitale (Du, Le-Khac, & Scanlon, 2017).

Kent, Chevalier, Grance, & Dang (2006) i përshkruajnë fazat themelore për kryerjen e kriminalistikës digjitale si më poshtë:

Mbledhja: identifikimi, etiketimi, regjistrimi dhe marrja e të dhënave nga burimet e mundshme të të dhënave përkatëse, përderisa ndjekin procedurat që ruajnë integritetin e të dhënave.

Ekzaminimi: përpunimi kriminalistik i të dhënave të mbledhura duke përdorur një kombinim të metodave të automatizuara dhe manuale, vlerësimi dhe nxjerrja e të dhënave me interes të veçantë duke ruajtur integritetin e të dhënave.

Analiza: analizimi i rezultateve të ekzaminimit, duke përdorur ligjërisht metoda dhe teknika të justifikueshme, për të nxjerrë informacion të dobishëm.

Raportimi: raportimi i rezultateve të analizës që mund të përfshijë përshkrimin e veprimeve të përdorura, shpjegimin e mënyrës së zgjedhjes së mjeteve dhe procedurave, përcaktimin e

veprimeve të tjera që duhen kryer (p.sh. ekzaminimin forenzik të burimeve shtesë të të dhënave, sigurimin e dobësive të identifikuara, përmirësimin e kontrolleve ekzistuese të sigurisë) dhe ofrimi i rekomandimeve për përmirësimin e politikave, mjetet e procedurave, dhe aspekteve të tjera të procesit kriminalistik.

Sipas Arnes (2018) procesi i forenzikës digjitale është i ndarë në 5-faza të njëpasnjëshme, por edhe përsëritëse, ku faza e parë është identifikimi i burimeve të mundshme të provave nga pajisjet digjitale; Pastaj, mbledhja e të dhënave digjitale duke kopjuar burimin; Tjetra, shqyrtimi i të dhënave të papërpunuara, duke u dhënë strukturë, kështu që është më e lehtë për t'u përpunuar dhe kuptuar; Pastaj analiza, ku kërkojmë të fitojmë një gjendje më të mirë dhe të identifikojmë objektet digjitale që në mënyrë ideale do të ishin prova dhe përfundimisht, i prezentojmë në një gjykatë ose në ndonjë njësi tjetër me interes, të paraqitur në grafikonin nr.1.

Grafikoni nr.1 Zinxhiri i proceseve dhe integriteti i provave

Burimi: Arnes, Andre (2018). Digital Forensics, John Wiley & Sons Inc.

Sipas, Arnes (2018) **identifikimi** i hapësirës ruajtëse të lëvizshme (ang. *removable storage*) duhet të sigurohet që së pari të kopjohen (ose "të klonohen") të dhënat e papërpunuara nga pajisjet para se të fillohet për kërkim të provave të krimit në fjalë. Për të siguruar që nuk ndryshohen të dhënat e ruajtura në pajisjet gjatë procesit të kopjimit, mund të përdoret modaliteti vetëm për lexim kur kemi qasje në të dhëna, nga ana tjetër, kjo mund të zbatohet edhe përmes softuerit ose pajisjeve që zakonisht njihen si teknologji të bllokimit të shkrimit (ang. *write-blocking*) (Arnes, 2018). Pas kopjimit, krijohet një nënshkrim digjital i hapësirës ruajtëse të lëvizshme (ang. *removable storage*) duke përdorur një funksion *hash* kriptografik,

duke llogaritur një nënshkrim digjital si për median origjinale ashtu edhe për kopjimin, e që mund të krahasohen për të verifikuar që përmbajtja është identike (Arnes, 2018). Të gjitha ndryshimet, të tilla si kopjimi, informacioni i çështjes dhe informacioni në lidhje me mënyrën se si është mbledhur dhe kush është përfshirë, duhet të dokumentohet. Mund të përdoren vegla të llojllojshme për të mbledhur të dhëna dhe për të gjeneruar një *hash* për të shmangur çdo pasiguri në mjetet e përdorura (si verifikimi i mjetit të dyfishtë), (Arnes, 2018).

Shumica e autorëve që e diskutojnë procesin e forenzikës përdorin termin mbledhje (**koleksionim**), ndërsa literatura më e orientuar teknikisht i referohet blerjes (ang. *acquisition*) ose nxjerrjes (ang. *extraction*), ku burimi tradicionalisht më i zakonshëm i provave kanë qenë *hard* disqet ose mediat e ruajtjes afatgjate të një kompjuteri, ndërsa përgatitja ose **ekzaminimi** është nxjerrja e provave të mundshme digjitale nga burimet e mbledhura të të dhënave (Arnes, 2018).

Në fazën e **analizës**, përmbajtja e *file*-ve të fituara të imazhit forenzik hetohet duke përdorur një sërë veglash për të kërkuar përmbajtje interesante brenda imazhit, ku *file*-t e fshehura, të fshirë dhe të koduar përkrah *IM chat logs*, historisë së shfletimit të internetit dhe postave elektronike të fshira mund të rikuperohen duke përdorur vegla të specializuara si *EnCase*, *Sleuth Kit*, *Volatility* dhe veglën e forenzikës (*FTK*), (Hassan, 2019). Përmbajtja e përgjithshme e raportit forenzik (**prezentimi**) duhet të përmbajë me sa vijon: një përmbledhje të gjetjeve kryesore; përshkrim i veglave (si harduerike ashtu edhe softuerike) të përdorura gjatë procesit të hetimit dhe funksionimit të secilit përveç versionit të mjeteve softuerike; metoda e përdorur për marrjen e provave digjitale; përshkrimi i provave digjitale (përmbajtja e imazhit) dhe artefakteve interesante të gjetura brenda tyre (p.sh., historia e shfletimit të internetit, historia e postës elektronike, analiza e regjistrit USB, *file*-t e fshirë). Gjithashtu është e preferueshme të përdoren kapjet e ekranit për t'i përshkruar hapat e ndërmarra; shpjegimi i termave teknikë të përdorur si "hapësira e pashpërndarë në disk" (ang. *unallocated disk space*) dhe të ngjashme, kështu që njerëzit joteknikë të mundet më lehtë ti kuptojnë termat teknikë të përmendur në raport nga përfundimi i hetimit (Hassan, 2019). Procesi i hetimit kompjuterik ndiqet nga 4 hapat sipas Prakash & Duhan (2020), e cila mund të përshkruhet si në: mbledhjen dhe ruajtjen e

provave, nxjerrja e provave, shqyrtimi i provave dhe organizimi i provave. Procesi digjital i forenzikës gjithashtu përfshin ekzaminimin dhe interpretimin e provave digjitale, ku ekzistojnë katër lloje të analizave që mund të kryhen në kompjutër, sipas Prakash & Duhan (2020):

a) Analiza e kornizës kohore;

b) Analiza e pronësisë dhe posedimit;

c) Analiza e aplikacionit dhe e *file*-it;

d) Analiza e fshehjes së të dhënave.

1.7 Gjurmimi i *hard*-disqeve

1.7.1 *Hard*- disqet dhe karakteristikat

Numri gjithnjë e në rritje i *hard*- disqeve është bërë kryesisht për shkak të avansimit rapid të teknologjisë, ku teknologjia e inspektimit vizual në industrinë e *hard* disqeve përfshin progresin dhe zhvillimet e fundit në teknologjinë e vizionit kompjuterik të *hard* disqeve (HDD) (Muneesawang & Yammen, 2015). Megjithëse depot e tyre (ang. *storage*) vijnë në shumë forma, *hard* disqet janë burimet më të pasura të provave digjitale mbi kompjuterët, ku edhe makinat moderne teknologjike kanë *hard* disqe dhe mund të lidhen me kontrollorët e jashtëm me një CPU, RAM, dhe *hard* disqe me kapacitet të lartë dhe të dhënat mund të ruhen, mund të fshihen dhe mund ti ndihmojnë hetuesit digjital të merren me *hard* disqet si një burim provash (Casey, 2011). HDD disqet-et janë në dy forma, fikse (të brendshme) dhe të jashtme, ku e para (fikse) ndodhet brenda pajisjes informatike, ndërsa HDD i jashtëm mund të lidhet me pajisjet informatike nëpërmjet një kablli USB ose eSATA (Hassan, 2019). Pajisjet HDD ruajnë të dhënat në pllaka, ku një *hard* disk mund të ketë një numër të caktuar të pllakave; Disqet me kapacitetet më pak se 500 GB do të përmbajnë vetëm një pllakë, ndërsa te disqet me kapacitete të mëdha, numri i pllakave mund të shkojë nga një deri në pesë, në varësi të madhësisë fizike të HDD-ve, kapacitetit, prodhuesit dhe modelit (Hassan, 2019). Kapaciteti i një disku të ngurtë mund të llogaritet duke shumëzuar numrin e cilindrave, kokave dhe sektorëve me nga 512 bajt (Casey,

2011). Të gjitha sistemet e *file*-ve që përdoren nga *Windows* organizohen nga *hard* disqe të bazuar në madhësinë e kllastereve (një kllaster përbëhet nga një numër sektorësh), ku madhësia e kllastereve përfaqëson sasinë më të vogël të hapësirës në disk që mund të përdoret për të mbajtur një *file* dhe varet nga sistemi i *file*-ve të përdorur dhe madhësia e një ndarjeje, dhe varion nga 4 në 64 sektorë (Hassan, 2019).

Sipas, (EC-Council, 2009) disa karakteristika që i dallojnë llojet e ndryshme të *hard* disqeve janë: **kapaciteti** i *hard* diskut, ndërfaqja (ang. *interface*-i) e përdorur, shpejtësia e rotacioneve në minutë, kërkimi në kohë, qasja në kohë dhe koha e transferimit; ndërsa sipas **dendësisë** të të dhënave në një *hard* disk ekzistojnë tri lloje: dendësia e pistave: (hapësira midis gjurmëve në një disk), dendësia e zonës: (numri i një *bit*-i për *inç* katror në një pjatë) dhe dendësia e një *bit*-i: (një *bit* për një njësi të gjatësisë së pistave). Dy faktorët më të zakonshëm të formave të HDD-ve bashkëkohorë janë 3.5-*inç* për kompjutorët desktop dhe 2.5-*inç* kryesisht për laptopët, ndërsa HDD-të janë të lidhura me sistemet me anë të kabllove standarde për *interface* si kabllot PATA (ATA paralele), SATA (*Serial* ATA), USB ose SAS (*Serial* bashkangjitur SCSI) (Zlatanov, 2015).

Në vitet e fundit, ngjashëm si me memorjen flash paraqiten edhe SSD-të, të cilat nuk kanë pjesë lëvizëse (ose pjata) dhe kursejnë të dhëna në një seri qelizash NAND *flash* ose mikroçipesh (NAND është i përbërë nga një grup tranzistorësh të ngjashëm me atë të përdorur në RAM; megjithatë, ky lloj tranzitori nuk ka nevojë të rifreskohet vazhdimisht në mënyrë që të ruajë të dhënat e tij, duke e bërë kështu një lloj të kujtesës jo të paqëndrueshme). SSD gjithashtu përdor një lloj kontrollori (i cili është një procesor i ngulitur) për të përcaktuar se si të ruhen, rigjehen dhe memorizohen të dhënat (Hassan, 2019). Sipas Hassan (2019), pavarësisht avantazheve të shpejtësisë, heshtjes dhe konsumit më të vogël të energjisë të llojit SSD, HDD-ja do të mbetet në përdorim të gjerë për shumë vite që do të vijnë, sepse kur fshini një *file* në një HDD, të dhënat e temës së *file*-it nuk do të fshihen menjëherë; në vend të kësaj, HDD do të fshijë vetëm treguesin në këtë *file*, duke shënuar hapësirën e tij në disk si të lirë dhe të dhënat e temës së *file*-it do të fshihen vetëm kur sistemi operativ duhet të shkruajë të dhëna të reja për vendndodhjen e tij.

1.7.2 Forenzika e *hard* disqeve

Një hetim tipik përfshin sekuestrimin e një *hard*- disku dhe mediave të tjera, të tilla si USB-të; bërja e kopjeve forenzike; vlerësimin e provave; dhe paraqitjen e një raporti. Për shembull, një analizë e forenzikës për një disk 6 TB mund të zgjasë disa ditë ose javë. Kjo do të thotë se duke u bazuar në përvojën e kaluar, menaxheri i laboratorit forenzik mund të vlerësojë se sa raste mund të trajtojë secili hetues dhe kur mund të presë një raport paraprak dhe përfundimtar për secilin rast (Nelson, Phillips, & Steuart, 2019). Pajisjet kompjuterike për ruajtje (ang.*storage*) (si *hard* disqet ose CD-ROM) mund të ruajnë ekuivalentin e miliona faqeve të informacionit. Për më tepër, një i dyshuar mund të përpiqet të fshehë provat penale; ai ose ajo mund ti ruajë atë në mënyrë të rastësishme me emra mashtrues të *file*-ve dhe kjo i determinon autoritetet e kërkimit për të shqyrtuar të gjitha të dhënat e ruajtura për të përcaktuar se cilat *file* të veçanta janë prova ose instrumente të krimit (Sammons J. , 2012).

Veglat e forenzikës lindën në DOS dhe me kalimin e viteve, Windows *hard* disqet përdorën një larmi *file*-sh, duke përfshirë FAT16, FAT32, sistemin e *file*-ve të teknologjisë së re (NTFS), sistemin e *file*-ve elastike (ReFS) dhe të tjerë, ku shumica e veglave të bazuara në DOS nuk mundën ti lexojnë disqet NTFS, përveç kësaj, popullariteti dhe përhapja e Xbox kërkonte që hetuesit të jenë të njohur me FATX sistemin e *file*-ve (Nelson, Phillips, & Steuart, 2019). Kjo do të thotë që për provat e ruajtura në një *hard* disk, ekzistojnë metoda të përcaktuara dhe praktikat më të mira për marrjen (ang. *acquiring*) dhe interpretimin e të dhënave. Kur merrni të dhëna nga një *hard* disk, është e rëndësishme të hiqni njësinë, ta lidhni atë me një kompjuter tjetër përmes një bllokuesi shkrimesh (ang. *write blocker*) dhe të bëni një kopje ekzakte *bit*-për-*bit* të *hard* diskut (Arnes, 2018). Furnizimi (ang. *acquisition*) fizik, i njohur gjithashtu si një imazh i *bit-stream*-it, në këtë metodë, gjenerohet një kopje *bit*-për-*bit,*sektor pas sektori të një *hard* disku (Hassan, 2019). Metadata e sistemit të *file*-ve, *file*-t e fshirë, fragmente të *file*-ve të fshirë dhe hapësira e papërcaktuar gjithashtu do të kapen duke përdorur këtë metodë, ku imazhi që rezulton do të jetë një dublikim i plotë i burimit (kopje e saktë); me fjalë të tjera, nëse po bëjmë një imazh të forenzikës së një *hard* disku prej 500 GB, imazhi që rezulton do të jetë saktësisht 500 GB, përveç nëse përdoret kompresimi gjatë procesit të furnizimit (ang. *acquisition*). Kjo është metoda më e përdorur në hetimin e të dhënave të kapura të cilat ruhen në një *file* imazhi,

ndërsa metoda e dytë është kopjimi i të të dhënave (*bit*-për-*bit*) nga disku burimor në një disk më të ri i cili ka të njëjtën kapacitet ruajtjeje ose pak më shumë (Hassan, 2019). Qasjet alternative përparojnë në një hap më tej, d.m.th., rindërtimi i plotë i imazhit të diskut në mënyrë të forenzikës së shëndoshë (ang. *forensically-sound*), gjegjësishtë në sistemin e propozuar, ku imazhi i të dhënave nuk arrihet përmes një kopje të tërë *bit*-për-*bit*, por ai i jep të njëjtin imazh të diskut forenzikisht të shëndoshë hetuesit (Du, Ledwith, & Scanlon, 2018). Rezultati i furnizimit (ang. *acquisition*) mund të verifikohet duke krahasuar *hash*-in e imazhit të rikrijuar të diskut me atë origjinal. Me qëllim të rindërtimit të imazhit në diskut, janë të nevojshëm tre përbërës të të dhënave binare, të cilat janë: të dhënat e *file*-it, hapësira e ngadaltë në nivelin e bllokut (ang. *block-level slack space*) dhe e treta është hapësira e pashpërndarë në disk, ku ky imazh i rindërtuar më pas mund të verifikohet kundrejt njësisë origjinale duke krahasuar vlerat e tyre të *hash*-it (Du, Ledwith, & Scanlon, 2018).

Një nxjerrje ose ekstrakcion fizik mund të kryhet duke përdorur kërkime të fjalëve kyçe bazuar në termat e dhëna të *file*-ve nga ana e hetuesit dhe duke ekzaminuar hapësirën e pashpërndarë, d.m.th., hapësirën e disponueshme në një sistem sepse nuk është përdorur kurrë ose sepse informacioni në të është fshirë. Nga ana tjetër nxjerrja logjike përfshin kërkimin dhe marrjen e provave nga situata në të cilën ndodhen në lidhje me sistemin e regjistrimit në një sistem operativ kompjuterik, i cili është përdorur për të ruajtur shënimet e emrave dhe të vendndodhjeve të *file*-ve që janë ruajtur në një pajisje ruajtjeje siç është *hard* disku (Prakash & Duhan, 2020).

Si duhet të veprojë hetuesi në nxjerrjen dhe ruajtjen e provave sipas (EC-Council, 2009) janë hapat e rradhës:

1. Dokumentacioni luan një rol kritik, ku hetuesi fillon hapin e parë duke shënuar informacionin e modelit nga etiketa e *hard* diskut dhe uebfaqja e prodhuesit, si dhe madhësinë dhe numrin e përgjithshëm të sektorëve në disk.

2. Hetuesi mund të vazhdojë më pas të përgatisë një imazh të *hard* diskut dhe për të siguruar që të gjitha të dhënat a janë fshirë nga disku dhe disku duhet të mbushet me zero.

3. Hapi tjetër është ndarja e diskut të sapo formatuar dhe rindezja.

4. Disku duhet të formatohet me sistemin e *file*-ve *ext3*.

5. Hetuesi pastaj përgatit diskun për imazhe përmes hapave të mëposhtëm: monton diskun e imazhit lexo-shkruaj; krijon një direktorium për të gjithë dokumentacionin dhe analizën; krijon një nëndrejtori për të mbajtur imazhin e dëshmisë; dokumenton detajet e hetimit në një *file* teksti, duke përfshirë detajet e hetuesit, detajet e çështjes, datat e hetimit dhe informacione të tjera rreth detajeve të dokumentit të medias së diskut. Duhet patur parasysh lidhjen e *hard* diskut që përmban strukturën e provave origjinale, verifikimin dhe sigurinë e sistemit.

6. Kontrollimi i saktësisë, montimi i diskut dhe nxjerrja e provave.

2. ASPEKTET ETIKE DHE LIGJORE TË FORENZIKËS DIGJITALE NË REPUBLIKËN E MAQEDONISË SË VERIUT

2.1 Aspektet etike dhe ligjore në forenzikën kompjuterike

Sipas Gogolin (2021) zhvillimet teknologjike në forenzikën digjitale ndodhin me një shpejtësi të madhe, ku hetuesit e forenzikës digjitale të sektorit privat duhet të kontaktojnë me zbatuesit e ligjit dhe të zhvillojnë një bashkëpunim sepse herët a vonë të dy rrugët do të gërshetohen. Sistemet digjitale të forenzikës mbledhin, filtrojnë, përpunojnë, ruajnë dhe shpërndajnë të dhëna, për të lehtësuar procesin e vendimmarrjes hetimore-organizative. Këto sisteme të specializuara përdoren për të vendosur dhe kuptuar specifikat e incidenteve elektronike. Për shkak se është një disciplinë e re, duhet të merren parasysh edhe faktorë të tjerë kontribues, sepse këto sisteme shkelin dhe sfidojnë shumë norma që janë bërë të pranueshme si nga individët ashtu edhe nga organizatat (Balogun & Zuva, 2017). Zbatimi i ligjit mund të mbështetet në prova digjitale për ndihmë nga një krim i pazgjidhur, ose gjithashtu mund të ketë raste kur hetimi zbulon qartë se ligjet janë thyer, por sistemi ligjor nuk pranon ta marrë çështjen në dorë. Nga ana tjetër shumica e agjencive të zbatimit të ligjit shpesh janë

jashtëzakonisht të nënfinancuara, gjë që çon në ngarkesa ekstreme të punës dhe ngarkesë të laboratorëve me më pak personel për të trajtuar një çështje, pra, praktikat e mira etike dhe praktikat e mira hetimore janë plotësuese kur i shikojmë gjërat nga një perspektivë tjetër analitike (Gogolin, 2021). Hetimet në forenzikën digjitale potencialisht kanë një efekt etik në çdo vendim të marrë. Në fakt kjo do të thotë që hetuesi digjital ka alternativën të vendosë se cilat prova do të hetojë, vërtetojë dhe të vendosë për thellësinë e analizës në çdo situatë të veçantë, por megjithatë, duhet të mbahet mend se hetuesi ka një obligim dhe, nëse një detyreë të tillë e anashkalojnë, ata mund të përballen me mundësinë e ndërmarrjes së veprimeve ligjore kundër tyre (Ironis & Konstadopoulou, 2007).

Atribuimi i krimeve kibernetike është i rëndësishëm në kufizimin e shkallës së krimit, si dhe në përgatitjen e nivelit të kërkuar të përgjigjes, sipas Shamsi, Zeadally, Sheikh, & Flowers (2016). Të motivuar nga kjo domethënie në qasjen e propozuar, atribuimi përbëhet nga tre hapa:

- identifikimi i armës kibernetike të përdorur;

- përcaktimi i origjinës së sulmit; dhe

- identifikimi i sulmuesit aktual.

Janë diskutuar disa nga çështjet ligjore që kanë të bëjnë me atribuimin, si dhe argumentojnë që ligjet ndërkombëtare të përcaktuara mirë për hapësirën kibernetike së bashku me bashkëpunimin e fortë midis qeverive janë të nevojshme për të gjetur dhe ndëshkuar kriminelët kibernetikë. Etika, sipas (Nelson, Phillips, & Steuart, 2019) janë rregullat që ne i përmbahemi dhe i përdorim për të matur performancën tonë; standardet që të tjerët i zbatojnë ndaj nesh, rregullat (kodet) e sjelljes, ose përgjegjësitë profesionale. Shumica e kriminalistëve punojnë në laboratorë të shkencës forenzike të lidhur me zbatimin e ligjit ose agjenci të tjera qeveritare që kanë kodet e etikës të zhvilluara posaçërisht për organizatat e tyre, ku kodet e etikës të zhvilluara për agjencitë prokuroriale adresojnë ato fusha të sjelljes profesionale që janë të rëndësishme për pjesën më të madhe të njerëzve (Barnett, 2001). Këshilli i Komisioinit Europian-është institucioni i parë që zhvilloi çertifikimin etik të hakerave (ang. *Certified Ethical Hacker*) ose (programi C|EH), ku qëllimi i këtij programi është të mësojnë metodologjitë, mjetet

dhe teknikat e përdorura nga hakerat, duke shfrytëzuar njohuritë kolektive nga qindra ekspertë të lëndës. Programi ka fituar shpejt popullaritet në të gjithë globin dhe tani ofrohet në më shumë se 70 vende nga më shumë se 450 qendra të autorizuara të trajnimit, si dhe në këtë kontekst janë trajnuar më shumë se 60,000 praktikues të informacionit (EC-Council, 2010). Sipas, rregullores së (Official Journal of the European Union, 2016) në lidhje me mbrojtjen gjatë përpunimit të të dhënave personale, definohet se identifikimi duhet të përfshijë identifikimin digjital të një subjekti të të dhënave, për shembull përmes mekanizmit të vërtetimit siç janë kredencialet e njëjta. Këto zhvillime kërkojnë një kornizë të fortë dhe më koherente për mbrojtjen e të dhënave në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente.

Analizat mund të parashikojnë polemika legjislative dhe politike që do të peshojnë të drejtat e qytetarëve për privatësinë dhe autonominë përkundrejt nevojave të shtetit për sigurinë nacionale dhe sigurinë publike (Losavio, Chow, Koltay, & James, 2018). Sfidat në analizën kriminalistike sipas Castillo (2019) janë: burimet e të dhënave, granuliteti i të dhënave, integriteti i të dhënave, të dhënat si prova ligjore, çështjet e privatësisë dhe analiza e të dhënave. Çështjet aktuale që dalin nga zhvillimi dhe implementimi i sistemeve të forenzikës digjitale i drejtojn hulumtimet e ardhshme të përqendrohen në adresimin e shqetësimeve që ato paraqesin për mirëqenien e një shoqërie, si: frika nga paparashikueshmëria, shkelja e privatësisë, shfrytëzimi i mjeteve, motivet tregtare dhe të ndarjes së tregut, standardizimi i praktikave dhe rezultatet e papërshtatëshme të edukimit dhe trajnimit (Balogun & Zuva, 2017).

2.2 Organizatat e kodeve të etikës të forenzikës digjitale

Përgjegjësitë e rregulloreve profesionale të kriminalistikës digjitale lihen në duart e enteve të ndryshme çertifikuese ose shoqërive profesionale të forenzikës digjitale (Sharevski, 2015), të cilat kanë rregullat e tyre për të drejtuar anëtarët e organizatës në fusha të ndryshme si: ndërveprimi me klientët, objektiviteti, roli në shoqëri, tarifat, pavarësia dhe marrëdhëniet kontraktuale (Nelson, Phillips, & Steuart, 2019). Duke u nisur nga ky këndvështrim sipas Nelson et. al., (2019) kodi i etikës dhe përgjegjësisë profesionale të Shoqërisë Ndërkombëtare të

Ekzaminuesve Kompjuteriko Ligjorë (ISFCE) ofron udhëzime për anëtarët e saj, ndërsa Shoqata Ndërkombëtare e Specialistëve të Hetimeve Kompjuterike (IACIS) ka një udhëzues mirë të përcaktuar dhe të thjeshtë për sjelljen e pritshme të ekspertëve të forenzikës.

Sipas (Sharevski, 2015) organizatat që lidhen me praktikën e forenzikës digjitale të kodeve të etikës janë: Akademia Amerikane e Forenzikës (AAFS); Bordi Amerikan i Kriminalistikës (ABC); Shoqëria Amerikane e Forenzikës Digjitale dhe e e-zbulimit (ASDFD); Shoqata e Kriminalistëve në Kaliforni (CAC); Konsorciumi i Specialistëve të Forenzikës Digjitale (CDFS); Instituti i Sigurisë Kibernetike (CI); Bordi i Certifikimit të Forenzikës Digjitale (DFCB); Këshilli i KE-së (ECC); Shoqata e Hetimit të Krimit të Teknologjisë së Lartë (HTCIA); Shoqata Ndërkombëtare e Specialistëve të Hetimit Kompjuterik (IACIS); Instituti SANS (SANS) dhe Shoqëria Ndërkombëtare e Ekzaminuesve Ligjorë Kompjuterik (ISFCE). Ekspertët e forenzikës duhet të kenë kujdes nga rregullat themelore të sjelljes profesionale që duhet ti ndjekin. Ata gjithsesi duhet të ndjekin modelin e kodit të përgjegjësisë profesionale dhe rregullat e modelit të sjelljes profesionale që janë kodet bazë të etikës së forenzikës digjitale (Nelson, Phillips, & Steuart, 2019). Ligjet e BE-së përqendrohen në çështjet e përbashkëta për mbrojtjen e privatësisë dhe sigurisë së besueshmërisë së provave dhe rezultateve, ndërsa në anën tjetër ndryshimi i katërt i Kushtetutës së SHBA-së ndalon kërkimet ose sekuestrimet e paarsyeshme të shtetit që janë në kundërshtim me ligjin, kur pa ndonjë shkak të mundshëm të një krimi, shkel privatësinë e qytetarëve (Losavio, Chow, Koltay, & James, 2018). Pfleeger (2015) potencon se me fuqi më të madhe vjen edhe përgjegjësia më e madhe. Ky koncept vlen edhe për kohërat e sotshme, ku teknologjitë e reja, qeveritë dhe organet rregullatore mund të ndërhyjnë për të vendosur strukturën, udhëzimet, standardet ose ndëshkimet mbi praktikën e sigurisë. Por, ndërhyrjet që tingëllojnë perfekte në teori nuk funksionojnë gjithmonë mirë në praktikë.

2.3 Analizat statistikore të krimit kompjuterik në Republikën e Maqedonisë së Veriut

Të dhënat statistikore për veprat penale nga krimet kompjuterike në Republikën e Maqedonisë së Veriut (RMV) janë siguruar nga databaza e Ministrisë për Punë të Brendshme (MPB), për periudhën kohore prej vitit 2010 deri në vitin 2019. Në tabelën nr.2 janë prezantuar llojet e krimit kompjuterik në vënd në përputhshmëri me "nenet" përkatëse nga Kodi Penal (KP) i Republikës së Maqedonisë së Veriut.

Tabela nr. 2 Mapa e krimeve kompjuterike

INKRIMINIMI LIGJOR NGA KODI PENAL I REPUBLIKËS SË MAQEDONIS SË VERIUT	
Nenet	***Llojet e krimeve kompjuterike***
neni. 144, fq.4	Rrezikimi i sigurisë
neni. 149, fq.2	Abuzimi i të dhënave personale
neni. 157, fq.2	Shkelja e të drejtës së autorit dhe të drejtave të lidhura me të
neni. 157-a	Shkelja e të drejtës së distributorit
neni. 157-b	Pirateria audiovizive
neni. 157-v	Fonogrami pirate
neni. 193	Shfaqja e pornografisë së fëmijëve
neni. 193-a	Prodhimi dhe shpërndarja e pornografisë së fëmijëve përmes një sistemi kompjuterik
neni. 193-б	Reduktimi i ngacmimeve seksuale tek fëmijët nën moshën 14 vjeç
neni. 251	Dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik
neni. 251-a	Krijimi dhe importimi i një virusi kompjuterik
neni. 251-b	Mashtrimi kompjuterik
neni. 271, fq.3	Krijimi, marrja ose tjetërsimi i fondeve të falsifikuara
neni. 394-g	Shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik
neni. 274-b	Bërja dhe përdorimi i një karte pagese false
neni. 379-a	Falsifikimi kompjuterik

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

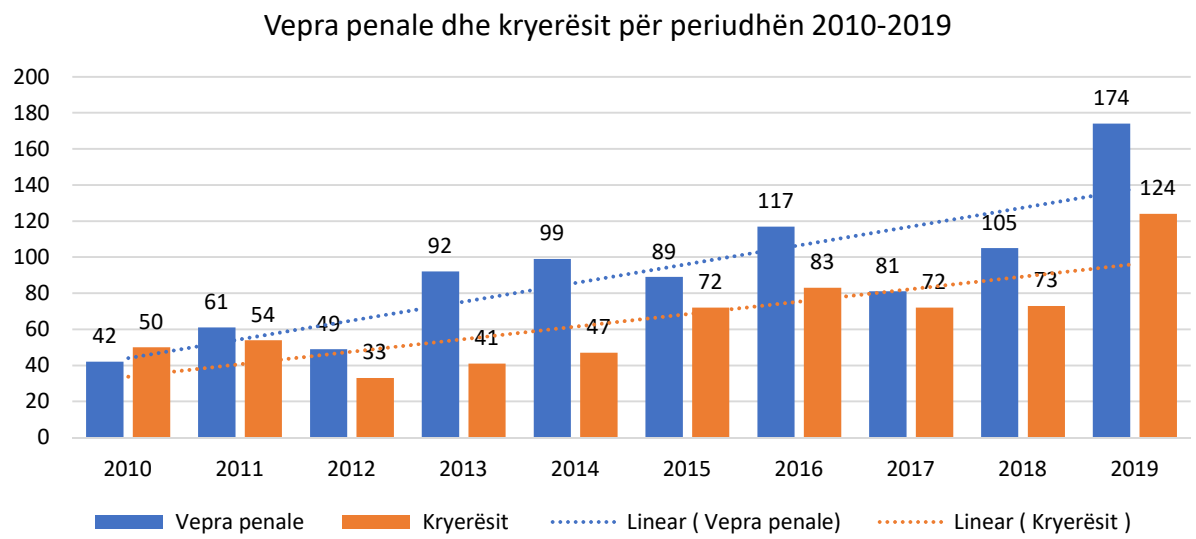
Veprat penale nga krimet kompjuterike për vitin 2010 ne RMV sipas Ligjit për Procedurë Penale (LPP) janë nenet: 251, 251-b dhe 379-a, ndërsa në vitin 2010 nuk u gjet asnjë vepër penale sipas nenit 274-b të Ligjit për Procedurë Penale. Për vitin 2011 ka të dhëna për veprat penale kompjuterike për nenet e ligjit penal: 251, 251-b dhe 274-b, ndërsa për nenin 379-a, gjegjësisht falsifikimi kompjuterik nuk janë gjetur të dhëna të veprës penale përkatëse. Në vijim në vitin

2012 janë regjistruar vepra penale për nenet përkatëse sipas (LPP): 251, 251-b, 274-b dhe 379-a. Për të njëjtat nene sipas Ligjit për Procedur Penale janë regjistruar shkelje ligjore, por të dhënat e njëjta të siguruara na MPB janë të strukturuara sipas Sektorëve për Punë të Brendshme (SPB) dhe sipas kriteriumeve në vijim: numërit të kryerësve, numërit të regjistrimeve të veprave penale, gjinisë dhe sipas moshës. Sipas (SPB) dhe kriteriumeve të mësipërme janë sigururar të dhëna edhe për vitin 2014. Për vitin 2015 janë siguruar të dhëna për kryerësit dhe veprat penale sipas (LPP) për nenet: 251, 251-b, 193-a, 149, 271 dhe 274-b. Gjatë viteve 2016 deri më 2019 vitin janë të siguruara të dhënat e të gjitha neneve përkatëse të (LPP) nga mapa e krimeve kompjuterike.

Struktura e analizave bazohet ne analogjine e kryerësve të krimeve kompjuterike dhe veprave penale për periudhën kohore 2010-2019. Analiza vazhdon me struktuimin e veprave penale dhe kryerësve sipas bazës ligjore dhe të difersifikuara në dy tabela të detajuara sipas të dhënave të disponueshme të veprave penale dhe kryerësve ndër vite. Në kontinuitet analizohet mesatarja e veprave penale sipas qyteteve (Sektoreve për Punë të Brendshëm) dhe përdorim ANOVA test në analizën përkatëse për vitet 2010-2014. Analiza e fundit i nënshtrohet hulumtimit me përdorimin gjithashtu të ANOVA testit duke analizuar mesataret dhe variancat sipas gjinisë dhe moshës dhe duke iu qasur analizës së moshës, me një përmbledhje në form të sintezës kumulative.

Në grafikonin nr.2 kemi shfaqur analogjinë dhe rrjedhjen e trendit në mes veprave penale dhe kryerësve gjatë viteve 2010-2019 në RMV. Karakteristike është se gjatë viteve 2011-2019 numri total i kryerësve është më i ulët se sa numëri total i veprave penale. Në anën tjetër numri më i lartë i veprave penale (174) dhe të kryerësve (124) është regjistruar në vitin 2019, ndërsa numëri kumulativ më i ulët është regjistruar në vitin 2012, gjithsejt (82). Karakteristikë e veçantë është se vërehet një trend linear gjatë viteve të hulumtimit, edhe ate se rrjedhja e lëvizjes së trendit pozitiv të veprave penale është më e lartë se sa rrjedhja e trendit pozitiv të kryerësve të krimeve kompjuterike në RMV.

Grafikoni nr.2 Vepra penale dhe kryerësit për periudhën 2010-2019



Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Shkaktarë të rritjes se veprave penale dhe kryerësve të krimeve kompjuterike në vend janë faktorë të ndryshëm. Si faktor kryesor është zhvillimi teknologjik, ndërsa determinantë tjetër është edhe rritja e përdoruesve të internetit në RMV gjatë kësaj periudhe kohore. Sipas të dhënave nga Banka Botërore (worldbank.org, 2021), numri i shfrytëzuesve të internetit (të shprehur si % e popullatës) ka një trend rritjeje në RMV, gjegjësisht duke nisur me (52%) në vitin 2010, (68%) gjatë vitit 2014 dhe të dhënat e fundit janë për vitin 2018 me (79%).

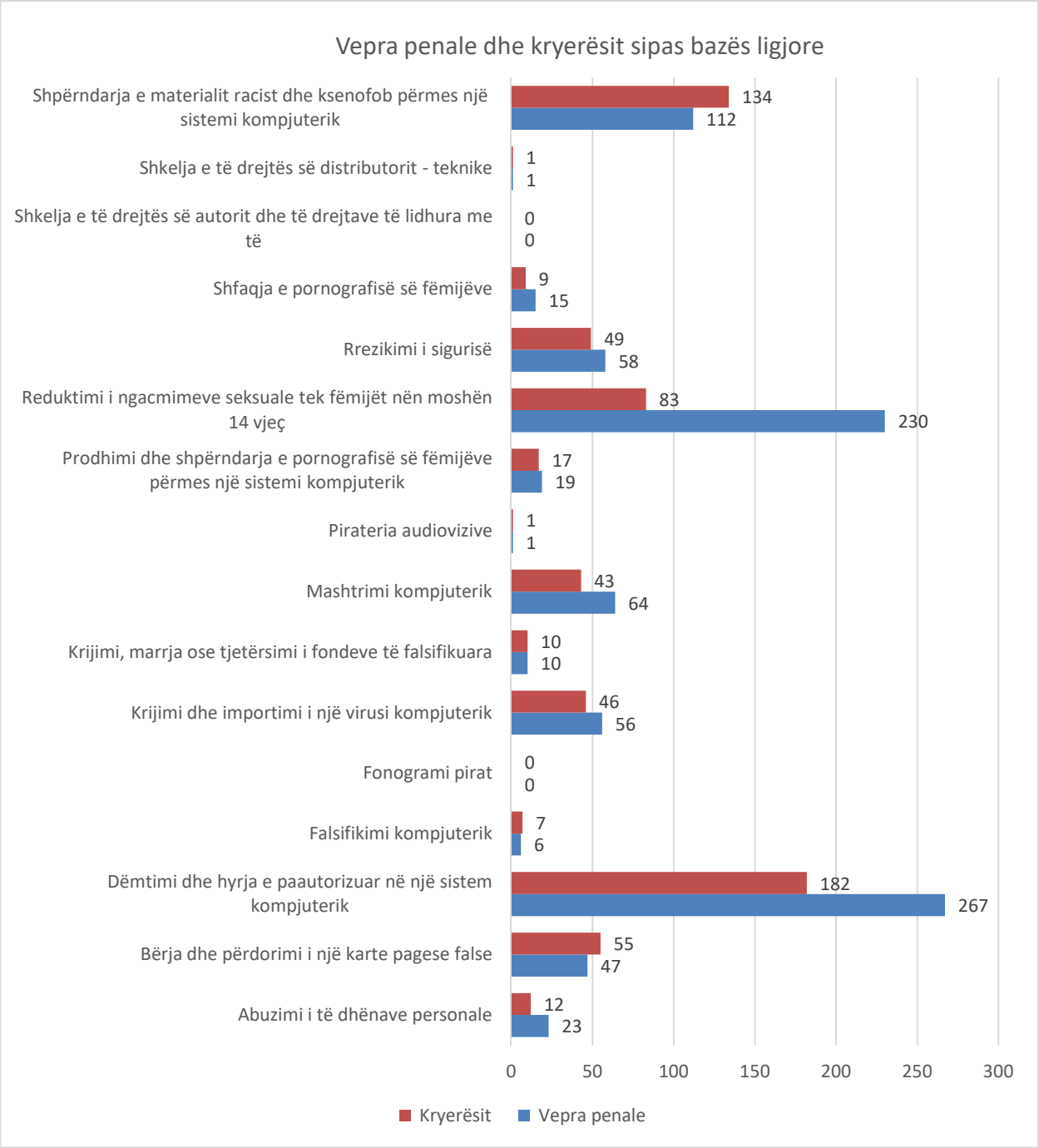
Në grafikonin nr.3 është paraqitur krahasimi në mes veprave penale të krimit kompjuterik dhe kryerësve sipas bazës ligjore. Numër më të madh të veprave penale (267) dhe të kryerësve (182) janë evidentuar sipas nenit-251 të Ligjit për Procedurë Penale, gjegjësisht “dëmtimit dhe hyrjes së paautorizuar në një sistem kompjuterik”.

Baza ligjore e dytë me më pak vepra penale dhe kryerësish të krimeve kompjuterike janë sipas kriteriumit ligjor “reduktimi i ngacmimeve seksuale tek fëmijët nën moshën 14 vjeç”, me (230) vepra penale dhe (83) persona që shfaqen si kryerës. Baza e tretë ligjore është “shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik” me (112) vepra penale gjatë periudhës 2010-2019, me (134) persona që janë regjistruar si kryerës. Në total, sipas veprave

penale dhe kryerësve me nga (107) shkelje ligjore dhe kryerje, janë regjistruar ato sipas bazave ligjore “rrezikim i sigurisë” dhe “mashtrim kompjuterik”. Ndërsa me nga (102) vepra penale dhe kryerje të krimeve kompjuterike janë evidentuar ato për kriteriumet ligjore: “krijimi dhe importimi i një virusi kompjuterik” dhe “bërja dhe përdorimi i një kartë pagese false”. Nga ana tjetër me më pak shkelje ligjore dhe numër të kryerësve (me më pak se 36-regjistrime), për gjatë viteve të hulumtimit, janë regjistruar ato sipas bazave ligjore: “prodhimi dhe shpërndarje e pornografisë së fëmijëve përmes një sistemi kompjuterik”, “abuzimi i të dhënave personale”, “shfaqja e pornografisë së fëmijëve”, “krijimi dhe marrja ose tjetërsimi i fondeve të falsifikuara”, dhe “falsifikimi kompjuterik”. Sipas “Shkeljes së të drejtës së distributorit” dhe “pirateria audiovizive” paraqiten me nga (1) vepër penale dhe numër të kryerësit. Sipas “shkeljes të së drejtës së autorit dhe të drejtave të lidhura me të” nga njëra anë dhe nga ana tjetër “fonogrami pirat” nuk është shfaqur shkelje ligjore sipas këtyre dy kriteriumeve.

Në analizën e detajuar të llojeve të krimeve kompjuterike në RMV gjatë periudhës kohore 2010-2019, karakteristike është se periudha prej vitit 2010 deri në vitin 2015 është më e ulët në krahasim me periudhën kohore prej vitit 2016 deri më 2019. Për atë shkak analiza është e dekompozuar në dy analiza për periudhat e lartëpërmendura. Faktor i dytë i shpërbërjes së tillë është edhe detirminanti kryesor se për një numër të madh të llojeve të krimeve kompjuterike nuk posedohet me të dhëna për periudhën kohore prej vitit 2010 deri në vitin 2015. Shkaktarët, për të cilat nuk posedohet me të dhëna për vitet 2010-2015, janë: rrezikimi i sigurisë, abuzimi i të dhënave personale, shkelja e të drejtës së autorit dhe të drejtave të lidhura me të, shkelja e të drejtës së distributorit, pirateria audiovizive, fonogrami pirat, shfaqja e pornografisë së fëmijëve dhe shpërndarja e pornografisë së fëmijëve përmes një sistemi kompjuterik (tabela nr.3). Llojet tjera te tabela nr.3, për periudhën përkatëse, kanë vlera të ulta të krimeve kompjuterike në krahasim me krimet e llojit të vet në vitet në vijim (prej vitit 2016 deri në vitin 2019). Me përjashtim të aktiviteve seksuale me një fëmije nën 14 vjeç, në veçanti janë regjistruar vepra të larta penale dhe kryerje të krimit të tillë kompjuterik gjatë viteve 2013 dhe 2014. Përjashtim i dytë gjatë viteve 2010-2015 është edhe shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik e cila karakterizohet me një regjistrim mesatar prej 21.75 të veprave penale dhe kryerjeve të krimeve kompjuterike gjatë viteve 2014-2015.

Grafikoni nr.3 Veprat penale dhe kryerësit sipas bazës ligjore, vitet 2010-2019



Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Tabela nr. 3 Llojet krimeve kompjuterike në periudhën kohore 2010-2015

Baza ligjore	2010		2011		2012		2013		2014		2015		TOTAL	
	Vepra penale	Krye rësit	Vepra penale	Krye rësit	Vepra penale	Krye rësit	Vepra penale	Krye rësit	Vepra penale	Krye rësit	Vepra penale	Krye ësit	Vepra penale	Krye rësit
Reduktimi i ngacmimeve seksuale tek fëmijët nën moshën 14 vjeç	0	0	47	29	31	14	74	16	76	22	0	0	**228**	**81**
Dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik	36	43	0	0	0	0	0	0	0	0	0	0	**36**	**43**
Krijimi dhe importimi i një virusi kompjuterik	0	0	1	2	7	5	4	1	4	5	40	33	**56**	**46**
Mashtrimi kompjuterik	5	6	0	0	0	0	0	0	0	0	8	3	**13**	**9**
Krijimi, marrja ose tjetërsimi i fondeve të falsifikuara	0	0	0	0	0	0	0	0	0	0	7	7	**7**	**7**
Bërja dhe përdorimi i një karte pagese false	0	0	0	0	1	1	1	0	1	0	7	6	**10**	**7**
Falsifikimi kompjuterik	1	1	0	0	0	0	0	0	0	0	1	0	**2**	**1**
Shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik	0	0	13	23	10	13	13	24	18	20	26	23	**80**	**103**
TOTAL	**42**	**50**	**61**	**54**	**49**	**33**	**92**	**41**	**99**	**47**	**89**	**72**	**432**	**297**

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Tabela nr. 4 Llojet krimeve kompjuterike në periudhën kohore 2016-2019

Baza ligjore	2016		2017		2018		2019		**TOTAL**	
	Vepra penale	Kryerësit	Vepra penale	Kryerësit	Vepra penale	Kryerësit	Vepra penale	Kryerësit	Vepra penale	Kryerësit
Rrezikimi i sigurisë	3	1	5	2	21	22	29	24	**58**	**49**
Abuzimi i të dhënave personale	1	1	1	1	2	0	19	10	**23**	**12**
Shkelja e të drejtës së autorit dhe të drejtave të lidhura me të	0	0	0	0	0	0	0	0	**0**	**0**
Shkelja e të drejtës së distributorit - teknike	0	0	0	0	1	1	0	0	**1**	**1**
Pirateria audiovizive	0	0	0	0	0	0	1	1	**1**	**1**
Fonogrami pirate	0	0	0	0	0	0	0	0	**0**	**0**
Shfaqja e pornografisë së fëmijëve	9	6	0	0	2	1	4	2	**15**	**9**
Prodhimi dhe shpërndarja e pornografisë së fëmijëve përmes një sistemi kompjuterik	7	5	4	6	2	1	6	5	**19**	**17**
Reduktimi i ngacmimeve seksuale tek fëmijët nën moshën 14 vjeç	0	0	2	2	0	0	0	0	**230**	**83**
Dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik	70	40	43	34	53	28	65	37	**267**	**182**
Krijimi dhe importimi i një virusi kompjuterik	0	0	0	0	0	0	0	0	**56**	**46**
Mashtrimi kompjuterik	12	3	13	12	14	10	12	9	**64**	**43**
Krijimi, marrja ose tjetërsimi i fondeve të falsifikuara	2	2	1	1	0	0	0	0	**10**	**10**
Bërja dhe përdorimi i një karte pagese false	13	25	12	14	4	2	8	7	**47**	**55**
Falsifikimi kompjuterik	0	0	0	0	1	3	3	3	**6**	**7**
Shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik	0	0	0	0	5	5	27	26	**112**	**134**
TOTAL	**117**	**83**	**81**	**72**	**105**	**73**	**174**	**124**	**909**	**649**

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Në tabelën nr.4 mund të vërehet se llojet e krimeve kompjuterike më të shprehura në RMV gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 janë:

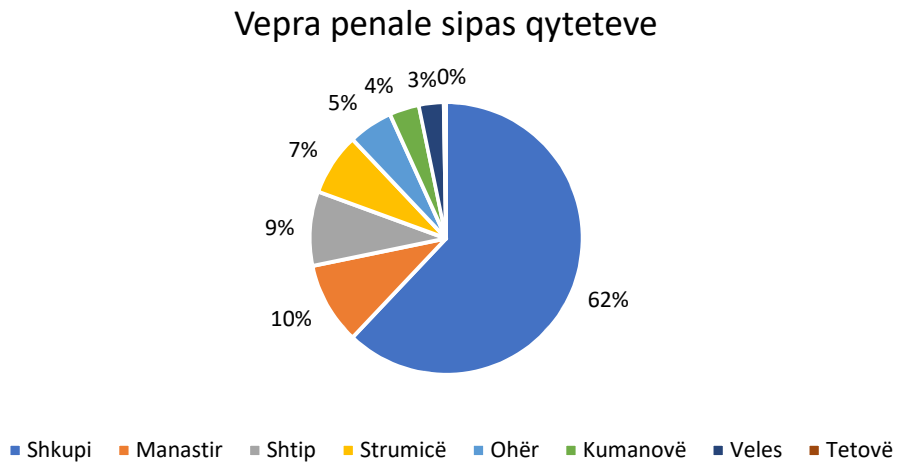
- **rrezikimi i sigurisë**, ku regjistrimet e veprave penale dhe kryerësve janë gjatë viteve 2018-2019 me një mesatare rreth 24 krime kompjuterike në vit;
- **abuzimi i të dhënave personale** si krim kompjuterik më i shfaqur paraqitet gjatë vitit 2019 me 19 vepra penale;
- **shfaqja e pornografisë së fëmijëve** më e lartë është regjistruar gjatë vitit 2016 me 6 kryerje dhe me 9 vepra penale;
- **prodhimi dhe shpërndarja e pornografisë së fëmijëve** përmes një sistemi kompjuterik - mesatarisht janë regjistruar rreth 6 vepra penale gjatë viteve 2016-2017 dhe gjatë vitit 2019;
- **dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik** gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 ndjek një mesatare me rreth 46 shkelje të paautorizuara gjatë një viti;
- **mashtrimet kompjuterike** që janë regjistruar gjatë viteve 2016-2019 janë me një mesatare rreth 11 veprash penale dhe kryerësish gjatë një viti;
- **bërja dhe përdorimi i një kartelë pagesore false** është e regjistruar si vepër penale me nivel më të lartë gjatë viteve 2016-2017 me një mesatare rreth 16 përdorimesh false të një kartele pagesore gjatë këtyre dy viteve; dhe
- **shpërndarja e materialit racist dhe ksenofob përmes një sistemi kompjuterik**, me një regjistrim më të lartë gjatë vitit 2019 me një mesatare rreth 27 vepra penale.

Në tabelën nr.5 janë prezentuar vlerat mesatare të krimeve sipas qyteteve gjatë periudhës kohore 2010-2014, ndërsa në grafikonin nr.4 janë prezentuar veprat penale sipas Sektorëve për Punë të Brendshme.

Gjatë periudhës së hulumtuar janë regjistruar 211 krime kompjuterike në qytetin e Shkupit, si qytet me popullatë më të dendur dhe popullim rreth 30% të popullatës totale nacionale dhe me vepra penale të krimit kompjuterik - rreth 62%. Në SPB-Shkup krimi më i shprehur është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik", për të cilin janë

evidentuar mesatarisht rreth 35 krime të realizuara, gjatë periudhës së hulumtuar. Vijon qyteti i Manastirit, për 4 vitet e hulumtuara, me 33 krime kompjuterike dhe 10% vepra penale të regjistruara; gjithashtu krimi më i frekuentuar është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik" me 5 krime të kryera. Sektori për Punë të Brendshme i qytetit të Shtipit rrenditet i treti sipas krimeve kompjuterike me 30 krime të regjistruara dhe 9% vepra penale, me mestare prej 4.2 krimesh dhe më i frekuentuari është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik". Në qytetin e Strumicës numri i krimeve kompjuterike është 25 krime për 4-vitet e hulumtuara dhe 7% vepra penale të regjistruara, edhe mesatarisht rreth 3.2 qasje të paautorizuara në një sistem kompjuterik si krim më i potencuar. SPB-Ohër shënon 18 krime dhe 5% të vepra penale nga totali i veprave penale sipas kriteriumit të diverzifikimit sipas qyteteve. Në qytetin e Ohrit krimi "dëmtim dhe hyrje e paautorizuar në një sistem kompjuterik" ndodh mesatarisht rreth 2.2 herë gjatë 4-viteve. SPB-Kumanovë karakterizohet me 12 krime kompjuterike, 4% vepra penale dhe mesatarisht 1.5 qasje të paautorizuara në një sistem kompjuterik, si dhe me njëmesatare të 1 përdorimi fals të një kartele pagesore. SPB-Veles regjistron 10 krime - 3% të veprave penale dhe mesatarisht 2 qasje të paautorizuara në një sistem kompjuterik. SPB-Tetovë regjistron vetëm 1 krim kompjuterik, gjegjësisht krimi i regjistruar është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik".

Grafikoni nr.4. Vepra penale sipas qyteteve



Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Tabela nr. 5. Numri mesatar i krimeve sipas Sektorëve për Punë të Brendshme), 2010-2014

Grupet	*Shuma*	*Mesatare*	*Varianca*
Shkupi	211	10.6	278.1
Manastir	33	1.7	4.8
Veles	10	0.5	1.0
Kumanovë	12	0.6	0.8
Ohër	18	0.9	1.5
Strumicë	25	1.3	6.9
Tetovë	1	0.1	0.1
Shtip	30	1.5	6.1

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

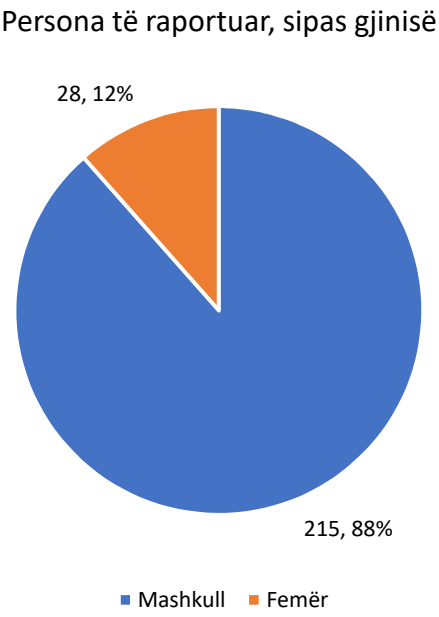
Me qëllim që të shqyrtohet nëse ekzistojnë ndryshime statistikore të rëndësishme midis Sektorëve për Punë të Brendshme në numrin mesatar të krimeve të kryera në periudhën prej 2010 deri në 2014, përdoret testi ANOVA. F-Statistikat të këtij testi janë 6.35 dhe që si e tillë përfaqëson një të dhënë statistikisht domethënëse, me një nivel domethënieje prej 0.05 (vlera e p-së është 0.000). Nëse SPB-Shkup përjashtohet nga analiza, si një sektor me shkallën më të lartë mesatare të krimeve të kryera, F-statistika është 2.23 dhe përsëri është statistikisht domethënëse në të njëjtin nivel rëndësie (vlera p është 0.044).

Tabela nr. 6 Personat e raportuar sipas gjinisë

Grupet	*Shuma*	*Mesatare*	*Varianca*
Mashkull	215	10.8	124.0
Femër	28	1.4	4.0

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Grafikoni nr.5 Pjesëmarrja e personave të raportuar sipas gjinisë



Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Nga numri i përgjithshëm i personave të raportuar në periudhën 2010-2014, 88% (ose 215 persona) janë meshkuj dhe 12% (ose 28 persona) janë femra, paraqitur në tabelën nr.6 dhe grafikonin nr.5. Pjesëmarrja e krimeve kompjuterike të kryera nga ana e meshkujve në raport me gjininë e kundërt është në raport 3 me 1 edhe pse kjo nuk korespondon me strukturën natyrale të numërit të gjinive të kundërta gjatë viteve 2010-2019 në RMV. Sipas raporteve të Treguesve të Zhvillimit Botëror (worldbank.org, 2021) gjatë viteve 2010-2019 në RMV, numri mesatar i popullatës sipas gjinisë femërore është 1.038.607 banorë, ndërsa sipas gjinisë mashkullore mesatarisht është 1.039.376 banorë, prej nga ku shihet se raporti natyror është i barabartë, ndërsa sa i përket raporteve të krimeve kompjuterike meshkujt prijnë trefish më shumë se sa gjinia femërore në RMV gjatë periudhës së hulumtimit.

Sipas moshës, shumica e personave të regjistruar në periudhën e përmendur janë midis 25 dhe 29 vjeç, të ndjekur nga personat e moshës 18-24 vjeç, të paraqitur në tabelën nr.7 dhe grafikonin nr.6. Krimet kompjuterike më të kryera nga personat midis moshës 25-29 janë: dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik, me 14 krime të kryera gjatë vitit

2010 dhe përdorimi i një kartele pagesore false - 10 krime gjatë vitit 2011. Personat e moshës 18-24 vjeç kanë kryer më së shumti 12-të dëmtime dhe hyrje të paautorizuar në një sistem kompjuterik gjatë vitit 2011 dhe 10-të krime të përdorimit të një karte pagese false gjatë vitit 2013.

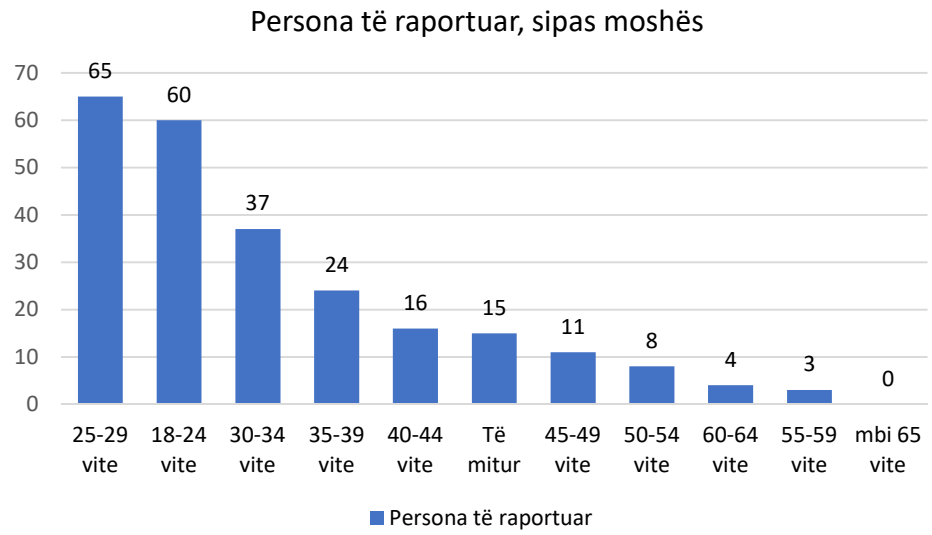
Tabela nr. 7 Personat e raportuar sipas moshës

Grupet	*Shuma*	*Mesatarja*	*Varianca*
Të mitur	15	0.75	3.14
18-24 vite	60	3	12.74
25-29 vite	65	3.25	16.51
30-34 vite	37	1.85	6.13
35-39 vite	24	1.2	3.54
40-44 vite	16	0.8	2.17
45-49 vite	11	0.55	1.63
50-54 vite	8	0.4	0.67
55-59 vite	3	0.15	0.13
60-64 vite	4	0.2	0.17
mbi 65 vite	0	0	0

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Nëse shikoni përqindjet kumulative (tabela nr.8), pak më shumë se 58% e personave të raportuar në periudhën e vëzhgimit janë nën 30 vjeç. Në vend të tretë sipas përqindjes mesatare, si pjesmarrës në krimet kompjuterike rrenditet grupi i moshës prej 30-40 vjeçe, me një pjesmarrje prej (15.2%) dhe që është karakteristike sepse me kumulativin paraprak të moshave nën 30 vjeç përbëjnë përafërsisht 73% prej totalit të krimeve kompjuterike në RMV për periudhën e hulumtimit.

Grafikoni nr. 6. Pjesëmarrja e personave të raportuar sipas moshës



Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Tabela nr. 8. Personat e raportuar sipas moshës (%-kumulative)

Mosha	***%***	***%-kumulativë***
Të mitur	6.2	6.2
18-24 vite	24.7	30.9
25-29 vite	26.7	57.6
30-34 vite	15.2	72.8
35-39 vite	9.9	82.7
40-44 vite	6.6	89.3
45-49 vite	4.5	93.8
50-54 vite	3.3	97.1
55-59 vite	1.2	98.4
60-64 vite	1.6	100.0
mbi 65 vite	0.0	100.0

Burimi: Ministria për Punë të Brendshme (MPB) të Republikës së Maqedonisë së Veriut

Dallimet në vlerat mesatare të numrit të personave të regjistruar sipas gjinisë dhe moshës janë statistikisht të rëndësishme në nivelin e domethënies prej 0,05. Statistikat F të testit ANOVA të kryer janë 13.66 dhe 5.98, përkatësisht për gjininë dhe moshën, ku vlera p në të dy rastet është e barabartë me zero.

2.4. Përfundimet

- Numri më i lartë i veprave penale (174) është regjistruar në vitin 2019, ndërsa karakteristikë e veçantë është se vërehet një trend pozitiv linear gjatë dekadës së fundit.
- Numër më të madh të krimeve kompjuterike sipas Ligjit për Procedurë Penale janë: "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik" me 267 vepra penale dhe dhe "ngacmimi seksual me një fëmije nën 14 vjeç", me 230 vepra penale.
- Llojet e krimeve kompjuterike më të shprehura në RMV gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 janë: rrezikimi i sigurisë; abuzimi i të dhënave personale; dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik i cili gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 ndjek një mesatare me rreth 46 shkelje të paautorizuara gjatë një viti, si dhe mashtrimet kompjuterike që janë regjistruar janë me një mesatare prej rreth 11 veprash penale gjatë një viti.
- Gjatë periudhës 2010-2014 janë regjistruar 211 krime kompjuterike në qytetin e Shkupit, ku krimi më i shprehur është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik", si te të gjitha SPB-të në RMV. Ndërsa sa i përket raporteve të krimeve kompjuterike, meshkujt prijnë trefish më shumë se sa gjinia femërore në RMV gjatë periudhës së hulumtimit. Sipas moshës, shumica e personave të regjistruar në periudhën e përmendur janë midis 25 dhe 29 vjeç, të ndjekur nga personat e moshës 18-24 vjeçare. Sipas përqindjeve kumulative, pak më shumë se 58% e personave të raportuar në periudhën e vëzhgimit janë nën 30 vjeç.

Gati është e pamundur të vlerësohet sasia e krimit kibernetik që ndodh në shumicën e kombeve në të gjithë botën për shkak të mungesës së përkufizimeve ligjore të standardizuara për këto vepra penale dhe disa statistikave zyrtare të vlefshme dhe të besueshme (Holt & Bossler, 2016). Sipas Indeksit Global të Sigurisë Kibernetike në Evropë (itu.int, 2017), i cili paraqet një analizë të Sigurisë Kibernetike për rajonin e Evropës, RMV rrezullton në nivelin mesatar sipas Indeksit Global të Sigurisë Kibernetike, gjegjësisht sipas raportit të shtyllave të mëposhtme:

- **Masat Ligjore**: bazuar në ekzistencën e institucioneve ligjore dhe kornizave që merren me sigurinë kibernetike dhe krimin kibernetik (**nivel i ulët**);

- **Masat Teknike**: bazuar në ekzistencën e institucioneve teknike dhe kornizave që merren me sigurinë kibernetike (**nivel i ulët**);

- **Masat Organizative**: bazuar në ekzistencën e institucioneve të koordinimit të politikave dhe strategjive për zhvillimin e sigurisë kibernetike në nivelin kombëtar (**nivel mesatar**);

- **Ndërtimi i kapaciteteve**: bazuar në ekzistencën e programeve kërkimore dhe zhvillimore, arsimore dhe trajnuese; profesionistë të çertifikuar dhe agjenci të sektorit publik që nxisin ndërtimin e kapaciteteve (**nivel i lartë**); dhe

- **Bashkëpunimi**: bazuar në ekzistencën e partneriteteve, kornizave bashkëpunuese dhe rrjeteve të shkëmbimit të informacionit (**nivel i lartë**).

3. FORENZIKA DIGJITALE, GJURMIMI I *HARD*-DISQEVE

Në këtë hulumtim, në korelacion me forenzikën e katër hard-disqeve te llojit Sata, kemi krijuar imazhet digjitale të katër hard-disqeve përmes softuerit FTK Imager. Imazhet e krijuara janë analizuar duke shfrytëzuar softuerin Autopsy 4.15.0.

Objektivat kryesore që janë shtjelluar në këtë kapitull janë: analiza e sfidave të forenzikës digjitale, gjurmimi i *hard*- disqeve, kthimi i fajlave të fshirë nga *hard*- disqet, cilësia e tyre pas kthimit, analiza e kthimit të fajlave nga *hard*- disqet e dëmtuara, si dhe rekomandimet për përmirësim në krahasim me teorinë dhe sistemet e reja të implementuara.

Siç e kemi potencuar edhe më parë, përdorimi i metodave të marra shkencërisht dhe të provuara për ruajtjen, mbledhjen, vërtetimin, identifikimin, analizimin, interpretimin, dokumentacionin dhe prezantimin e provave digjitale, të marra nga burimet digjitale me qëllim të lehtësimit ose avancimit të rindërtimit të ngjarjeve të cilat konsiderohen kriminale ose ndihmës për të parashikuar veprime të paautorizuara, janë treguar si shqetësuese për operacionet e planifikuara. (Frauenhoffer, 2018)

Forenzika digjitale merret më së shumti me rastet për të përpunuar dhe analizuar provat digjitale të mbledhura nga skenat e krimit. Procesi i punës në një rast të forenzikës digjitale përfshin krijimin e imazhit të diskut (kopjet e paisjes së të dyshuarit origjinal), *hash*-imin ose verifikimin e integritetit të figurës së diskut, bën bllokimin e figurës së diskut (vendosjen e tij vetëm për të lexuar për të verifikuar integritetin e figurës së diskut), analizimin e diskut dhe përmbajtjen e tij. (Frauenhoffer, 2018)

Në këtë studim është shfrytëzuar vegla FTK Imager, me ndihmën e të cilit janë krijuar imazhet e katër hard- disqeve të testuara.

FTK Imager është vegël pa pagesë nga AccessData.com, e cila shfrytëzohet si një vegël që përdoret për të krijuar një kopje të saktë të një *hard*- disku ose pajisje tjetër (CD, USB, etj.), me qëllim të analizës gjatë një hetimi. Është *hex* inspektues (ang. *hex viewer)* dhe llogaritet edhe si vegël për *hash*-im duke siguruar edhe interpretim të të dhënave. (AccessData Group, Inc, 2017)

3.1 Ç'ka paraqet imazhi i një disku?

Imazhet e diskut përdoren për të transferuar përmbajtjen e një hard- disku për arsye të ndryshme. Imazhi i një disku mund të përdoret në disa raste, duke përfshirë: rivendosjen e përmbajtjes së një disku gjatë rimëkëmbjes së tij, transferim i përmbajtjes së një hard- disku nga një kompjuter në tjetrin, ose për të rivendosur përmbajtjen e një hard- disku pas azhurimit ose riparimit të harduerit. Për më tepër, ai mund të përdoret për të krijuar një kopje të saktë të një *hard*- disku ose pajisje tjetër (CD, USB, etj.) me qëllim të analizës gjatë një hetimi.

Imazhi i një disku përcaktohet si një *file* kompjuterik që përfshin përmbajtjen dhe strukturën e një pajisje për ruajtjen e të dhënave siç është hard disku, CD- disku, telefoni, tableti, RAM ose USB. Imazhi i diskut përbëhet nga përmbajtja aktuale e pajisjes për ruajtjen e të dhënave, si dhe informacionin e nevojshëm për të përsëritur strukturën dhe paraqitjen e përmbajtjes së pajisjes.

Kjo ndryshon nga një kopje reserve (*backup*) normale sepse në atë, integriteti i strukturës së saktë të ruajtjes mbetet i paprekur, gjë që është thelbësore në ruajtjen e integritetit të një gjurmimi (investigimi) forenzik.

Nëse struktura e dokumentacionit të përgaditur (dosjes) dhe përmbajtja e saj nuk mund të verifikohen se janë saktësisht të njëjta me modelin origjinal të synuar, integriteti i provave është në rrezik dhe mund të jetë i papranueshëm në një proces gjyqësor. (Frauenhoffer, 2018)

Një imazh mund të merret në vend ose nga distanca. Në rastin kur një imazh i diskut bëhet në vend, ruajtja e të dhënave është fizikisht e disponueshme, siç është USB ose hard- disku i një kompjuteri të disponueshëm.

Në rastin e krijimit të imazhit nga distanca, pajisja e ruajtjes së synuar nuk është e pranishme (p.sh një kompjuter në zyrën e një të dyshuari në vendin e tij të punës).

Ekzistojnë softuere të ndryshëm që janë specifikuar posaçërisht për njërin apo procesin tjetër. Në këtë punim kemi bërë hulumtimin e imazheve të katër *hard*- disqeve eksterne duke përdorur FTK Imager. FTK Imager është një softuer pa pagesë i krijuar nga kompania *AccessData* dhe ka për qëllim krijimin e imazheve lokale dhe atyre të largëta (ang. *remote*). (Frauenhoffer, 2018)

3.2 Ekzaminim i provave digjitale

(ang. *About Examining Digital Evidence*)

Analizimi i provave është një proces për të gjetur dhe identifikuar të dhëna domethënëse, për t'i vënë ato në dispozicion të palëve dhe më lehtë për t'u kuptuar. Pasi të përfundon instalimi dhe të krijoni një rast (ang. *case*), mund të shtoni provën si dëshmi për analizë. Prova mund të përfshijë imazhe të disqeve të ngurtë, CD dhe DVD, mjete portative siç janë USB, dhe/ose të dhëna të drejtpërdrejta (pa imazhe) nga çdo burim elektronik i zakonshëm.

3.3 Krijimi i imazheve digjitale te *hard*-diksut 1, 2, 3 dhe 4 përmes FTK Imager

Siç cekëm edhe me lartë, imazhi forenzik është më së shpeshti i nevojshëm për të verifikuar integritetin e imazhit pasi të ketë ndodhur një përvetsim i një hard- disku. Kjo si zakonisht

shërben si dëshmi në bazë të nevojës në gjykatë sepse, pasi të jetë krijuar një imazh kriminalistik, integriteti i tij mund të kontrollohet për të verifikuar që nuk është ndërhyrë në te. Më tej, një imazh forenzik mund të rezervohet dhe/ose të testohet pa e dëmtuar kopjen ose provën origjinale.

Ka shumë mënyra për të krijuar një imazh forenzik. Këtu kemi përdorur veglën e mirënjohur FTK Imager për Windows, për të krijuar imazhe të hard-disqeve me të cilat kemi eksperimentuar.

Paisjet harduerike të cilat janë shfrytëzuar për realizimin e krijimit të imazheve forenzike janë Tableau eSata Forensic Bridge, *hard*-disku 1, *hard*-disku 2, *hard*-disku 3 dhe *hard*-disku 4 dhe të cilët janë paraqitur më poshtë.

Paisja *Tableau eSata Forensic Brige* është një bllokues i lëvizshëm portativ (ang. *portable*) i të shkruarit që mundëson përvetësimin forenzik të *hard*-disqeve SATA.

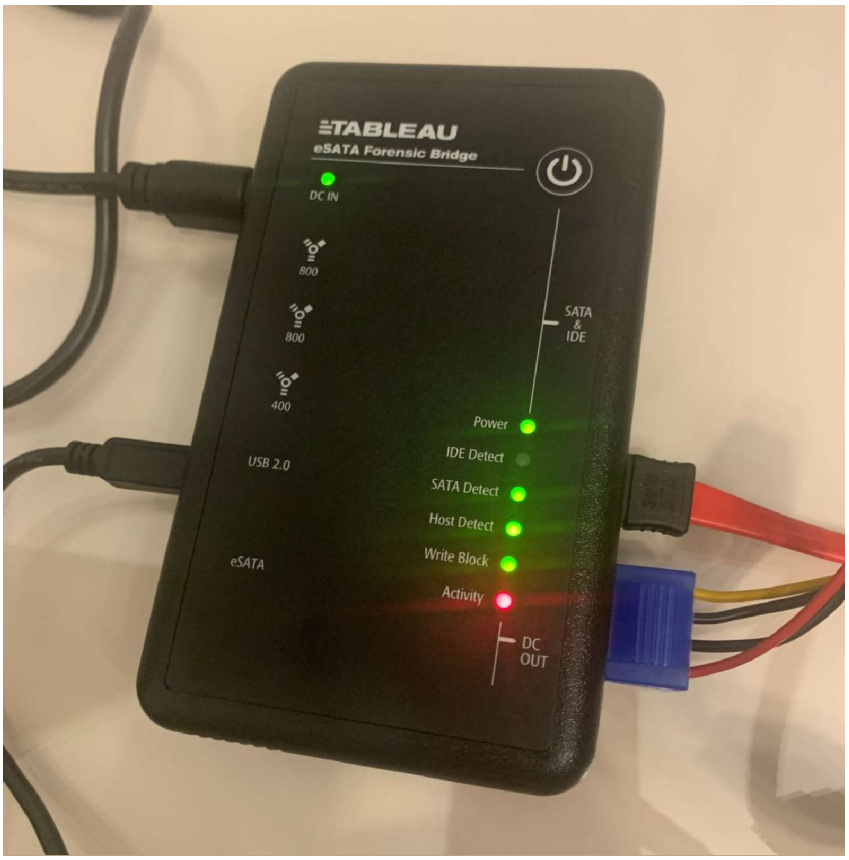


Fig. 1 Tableau eSata Forensic Bridge

Nga figura më lartë mund të vërejmë se kur paisja Tableau eSata Forensic Brige është e kyçur sinjalizon dritën e gjelbërt tek sinjalizuesi *power*, pasi *hard*-disqet që i kemi testuar janë të llojit SATA dhe prandaj e sinjalizon atë me të gjelbërt - SATA power. *Host detect* sinjalizon me të gjelbërt kur paisja Tableau detekton kompjuter të lidhur me paisjen në fjalë ndërsa kur *Write Block* është aktiv, ai na siguron se në *hard*-diskun të cilin e kopjojmë për të krijuar një imazh forenzik, nuk është ndryshuar asgjë dhe se qasja ndaj atij hard-disku ka qenë vetem leximi dhe kopjim i të dhënave (read-only) në kompjuterin tonë si dhe na siguron që mundësia (opsioni) për ndërhyrje në *hard*-diskut është i blokuar. Sinjalizimi me dritë të kuqe tek *Activity* tregon që paisja për momentin është aktive.

Hard- disku 1, siç mund të shihet në figurën e mëposhtme, posedon këto karakteristika:

- Numri serik: WD-WMAM9SL03689
- Tipi: SATA
- Kapaciteti: 80 GB.

Specifikacioni I hard-diskut 1	
Numri serik	WD-WMAM9SL03689
Numri i modelit	WD800JD – 75MSA3
Emri i modelit	Caviar SE
Kapaciteti i diskut	80 Gbytes
Shpejtësia e rrotacioneve (ang. *Rotational Speed)*	7,200 rpm
Madhësia (ang. *Form Factor width*)	3.5-inch
Madhësia e *bafeirt* (ang. Buffer Size)	8 MB
Lloji (ang. *Enclosure Type*)	INTERNAL

Vendor: WDC WD80 Model: 0JD-19JN Revision: 1C05 Serial Number: WD-WCAM96993422 Bus: SATA

Fig. 2 Hard-disku 1

Hard- disku 2, siç mund të shihet në figurën e mëposhtme, posedon këto karakteristika:

Specifikacioni I hard-diskut 2	
Numri serik	WD-WMAM9SP32232
Numri i modelit	WD800JD – 75MSA3
Emri i modelit	Caviar SE
Kapaciteti i diskut	80 Gbytes
Shpejtësia e rrotacioneve (ang. *Rotational Speed)*	7,200 rpm

Madhësia (eng.*Form Factor width*)	3.5-inch
Madhësia e *baferit* (ang. *Buffer Size*)	8 MB
Lloji (ang. *Enclosure Type*)	INTERNAL

Fig. 3 Hard-disku 2

Hard- disku 3, siç mund të shihet nga figura e mëposhtme, posedon këto karakteristika:

Specifikacioni I hard-diskut 3	
Numri serik	WD-WMAM9SL61446
Numri i modelit	WD800JD – 75MSA3

Emri i modelit	Caviar SE
Kapaciteti i diskut	80 Gbytes
Shpejtësia e rrotacioneve	7,200 rpm
Madhësia fizike	3.5-inch
Madhësia e *baferit* (ang. Buffer Size):	8 MB
Lloji (ang. *Enclosure Type*):	INTERNAL

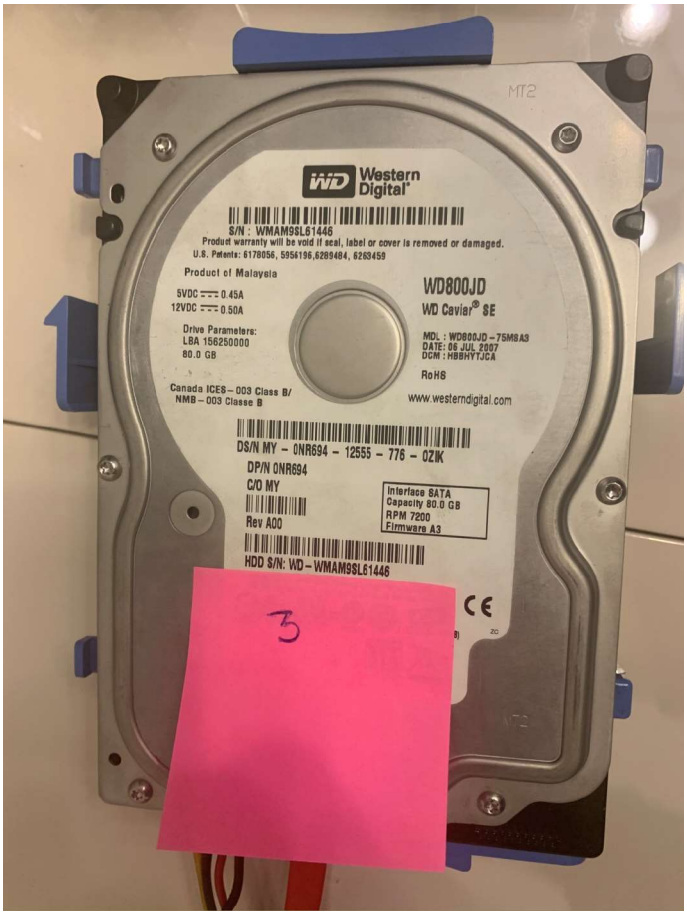


Fig. 4 Hard-disku 3

Hard- disku 4, i paraqitur në figurën e mëposhtme, posedon këto karakteristika:

Specifikacioni I hard-diskut 4	
Numri serik	WD-WMAM9SF02255
Numri i modelit	WD800JD – 75MSA3

Emri i modelit	Caviar SE
Kapaciteti i diskut	80 Gbytes
Shpejtësia e rrotacioneve (ang. *Rotational Speed)*	7,200 rpm
Madhësia (ang. *Form Factor width*)	3.5-inch
Madhësia e *baferit* (ang. Buffer Size)	8 MB
Lloji (ang. *Enclosure Type*)	INTERNAL

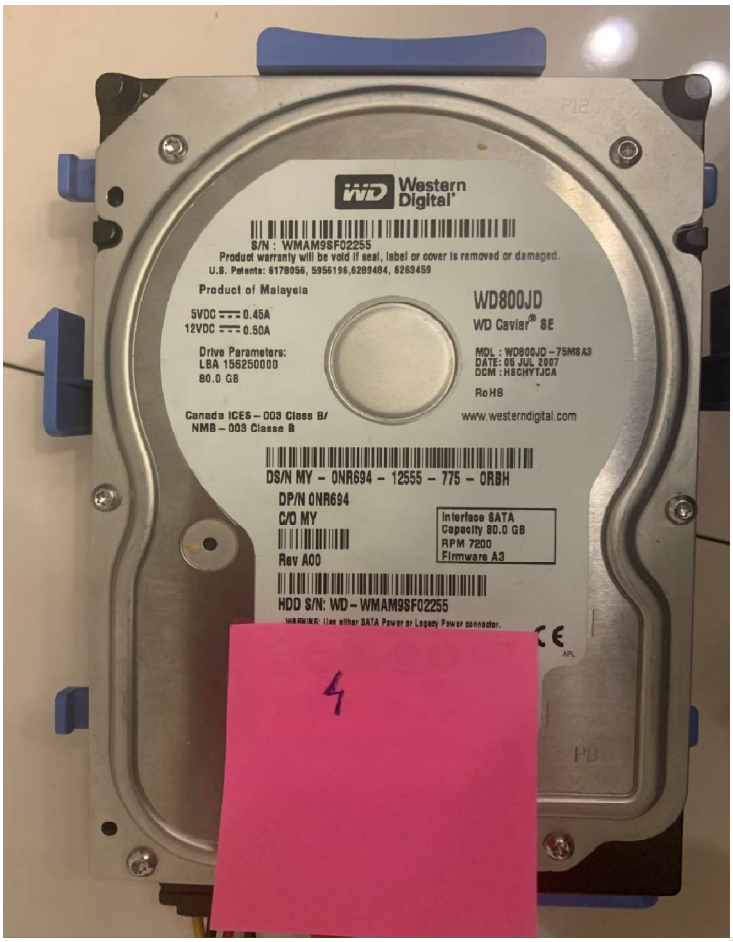


Fig. 5 *Hard*-disku 4

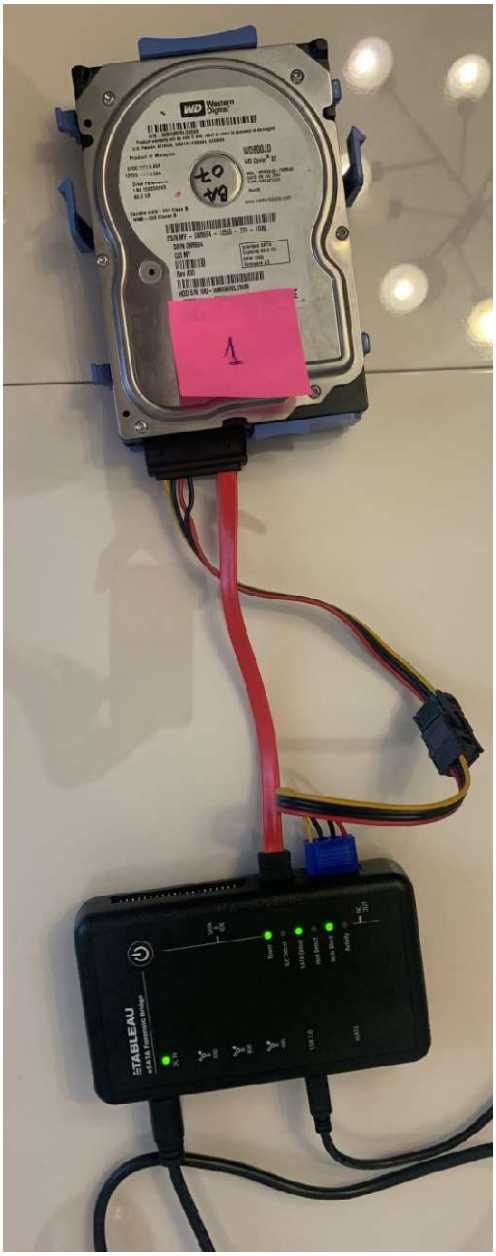


Fig. 6 Ndërlidhja e *hard*-diskut me paisjen Tableau

Krijimi i FTK imazheve u bë në disa etapa të cilat do të mund ti shihni në vijim:

Në fillim, pasi hapet aplikacioni *FTK Imager*, shkohet në *menu bar* dhe klikohet në *File* - ku përzgjidhet *Create Disk Image* për të krijuar imazhin e hard-diskut të lidhur fizikisht me PC-në apo laptopin.

Krijim i imazhit të diskut përmes FTK Imager 4.3.1.1

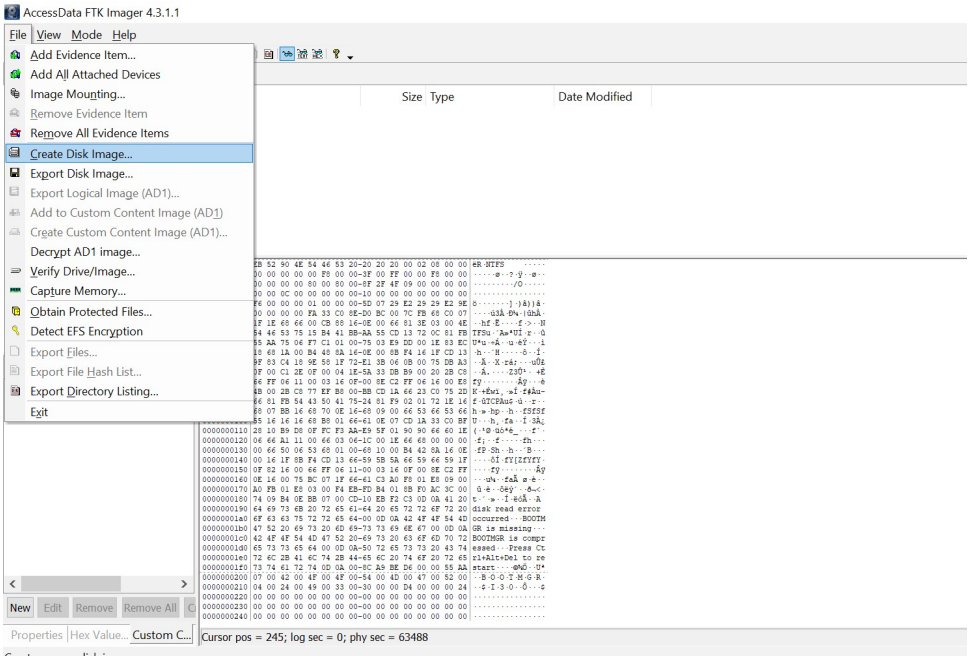


Fig. 7 Krijim i imazhit të diskut përmes FTK Imager 4.3.1.1

Pastaj na shfaqet dritarja komunikuese '*Select Source'* ku përzgjedhim *'Physical drive',* në qoftë *se* kemi lidhur një *hard*- disk fizik me kompjuterin që po përdorim për të bërë imazhin forenzik.

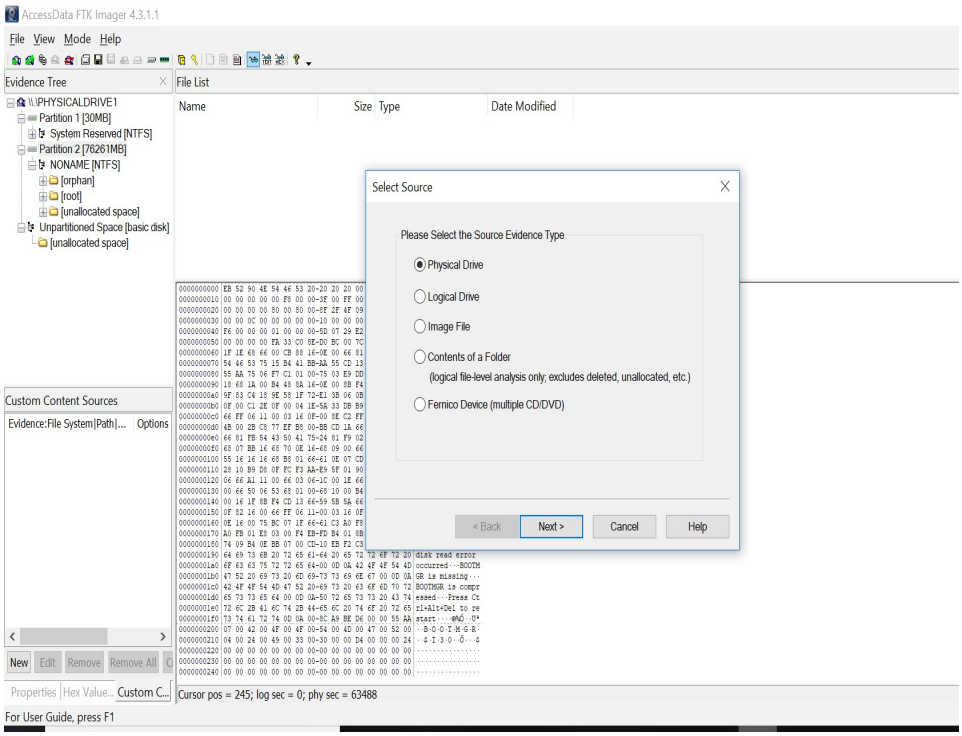


Fig. 8 Përzgjedhja e opcionit disku fizik *(ang.physical drive)* gjatë krijimit të imazhit të diskut

Pastaj bëhet përzgjedhja e *hard*- diskut për të cilin krijohet imazhi forenzik.

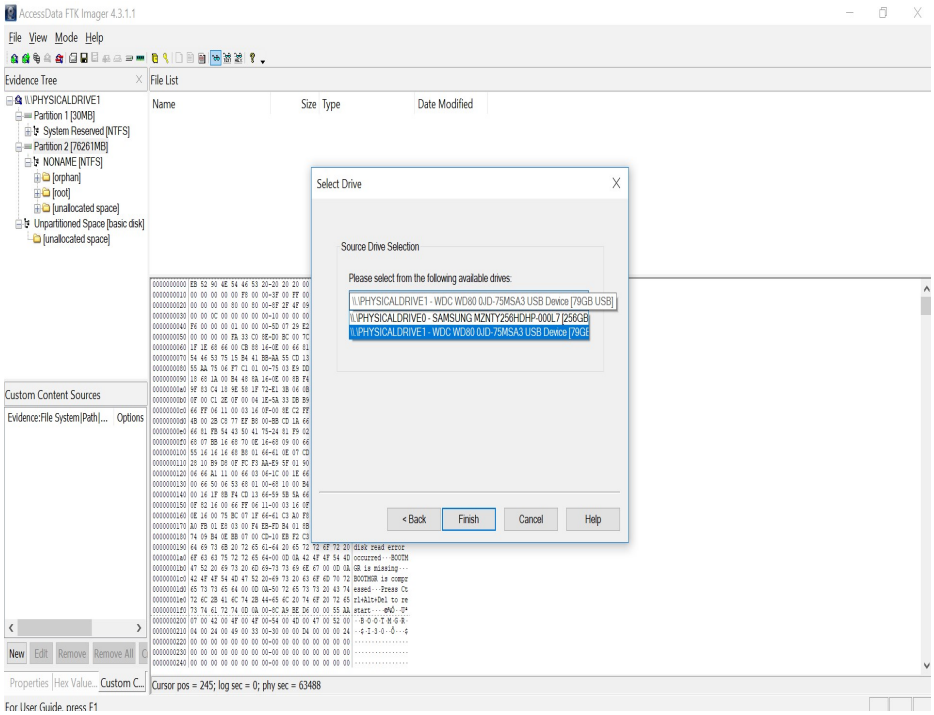


Fig. 9 Përzgjedhja e hard-diskut për të cilin krijohet imazhi

Më pastaj bëhet destinimi i imazhit të diskut që do të krijohet:

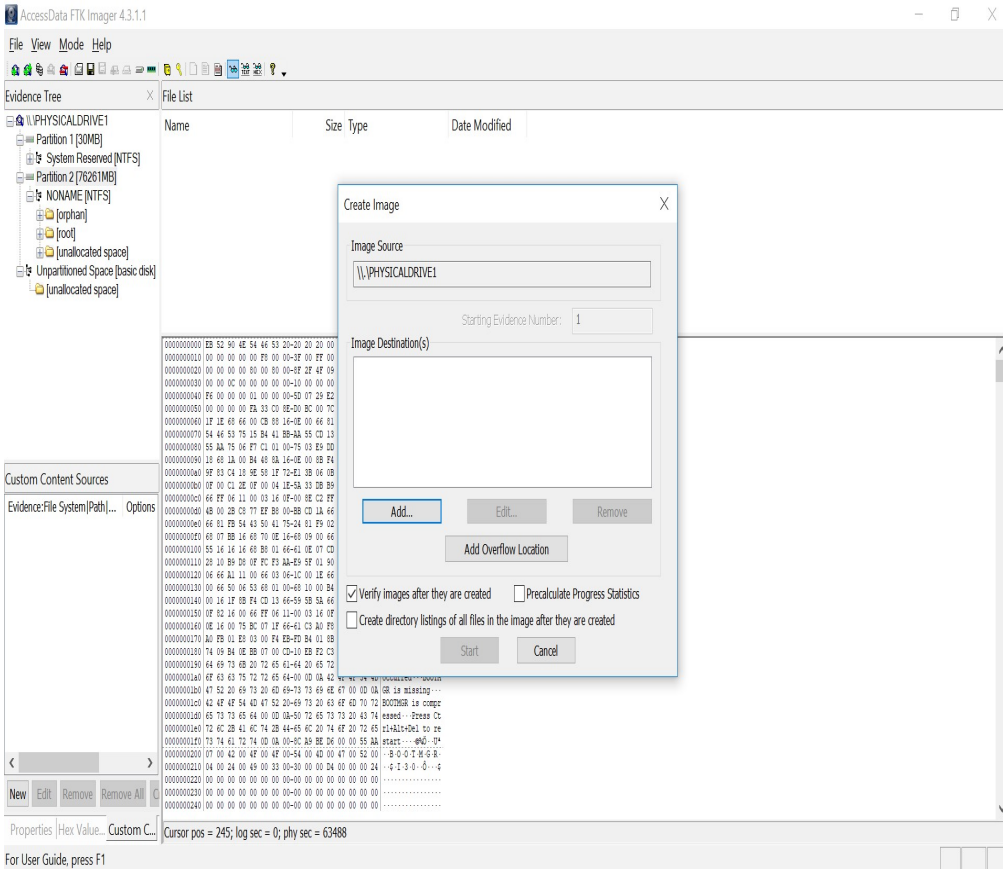


Fig. 10 Destinimi i imazhit që krijohet

Me përzgjedhjen e E01 përcaktohemi për zgjedhjen e llojit të imazhit që do të krijohet. Si zakonisht preferohet E01 për shkak të verifikimit të *hash*-it dhe aftësisë së tij për t'u përdorur me shumë programe të tjera.

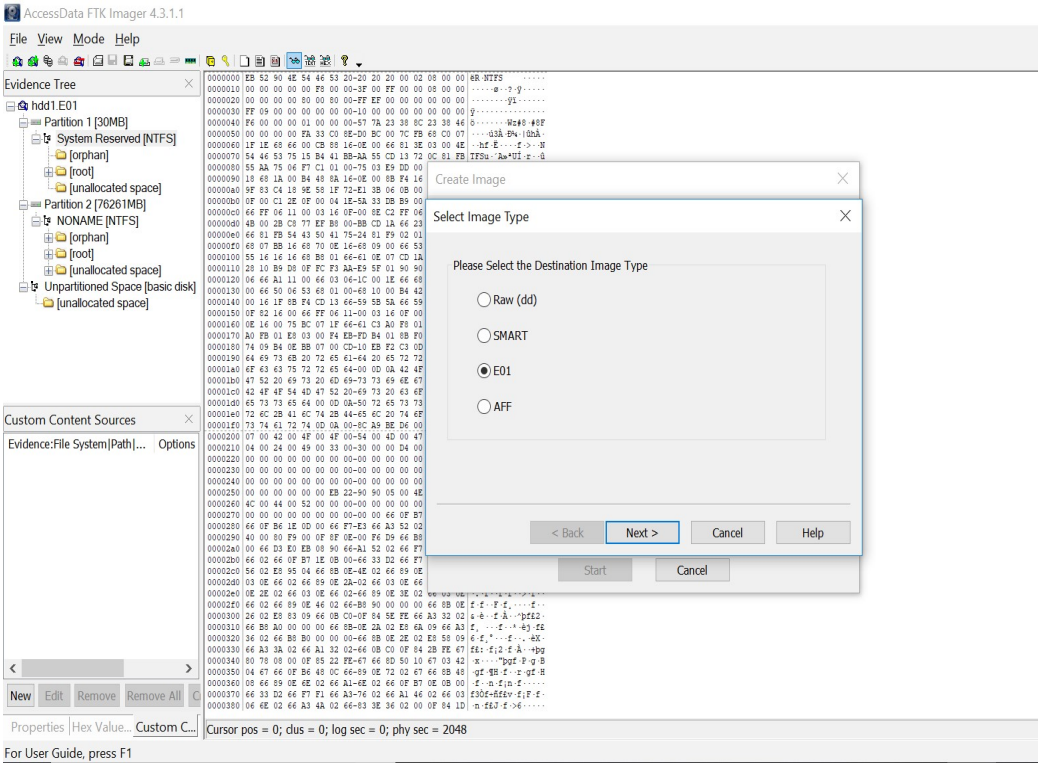


Fig. 11 Përzgjedhja e llojit të imazhit që do të krijohet

Më poshtë shihet plotësimi i të dhënave gjatë gjenerimit të imazhit të diskut. Çdo herë duhet patur kujdes me të dhënat që plotësohen në këtë dritare, pasi i njëjti material do të shërben në procese gjyqësore.

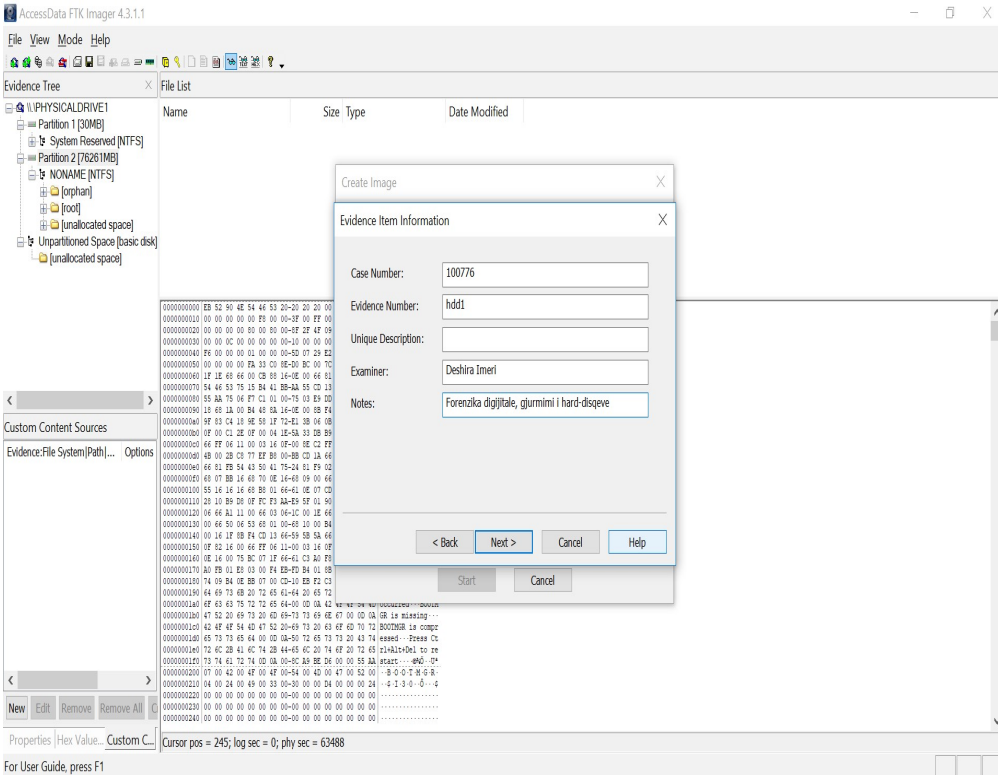


Fig. 12 Plotësimi i të dhënave gjatë gjenerimit të imazhit të diskut

Gjithashtu, duhet të zgjedhim destinacionin ku dëshirojmë të eksportojmë imazhin forenzik duke i caktuar imazhit një emër.

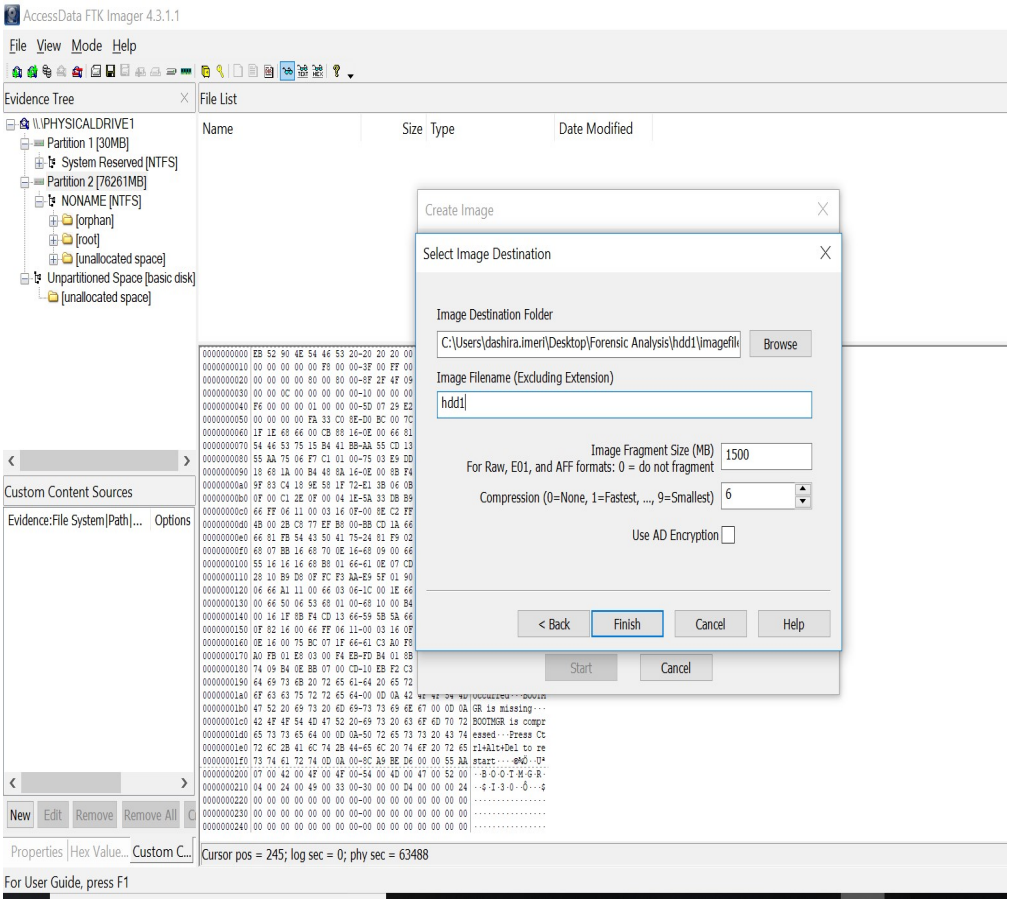


Figure 13 Pëzgjedhim destinacionin ku dëshirojmë të eksportojmë imazhin forenzik

Në vazhdim duhet të presim që imazhi forenzik të krijohet dhe pastaj të verifikohet. Pasi të kenë ndodhur të dy proceset, mund të vazhdohet me softueret tjera për testime të imazheve të krijuara sic është Autopsy etj.

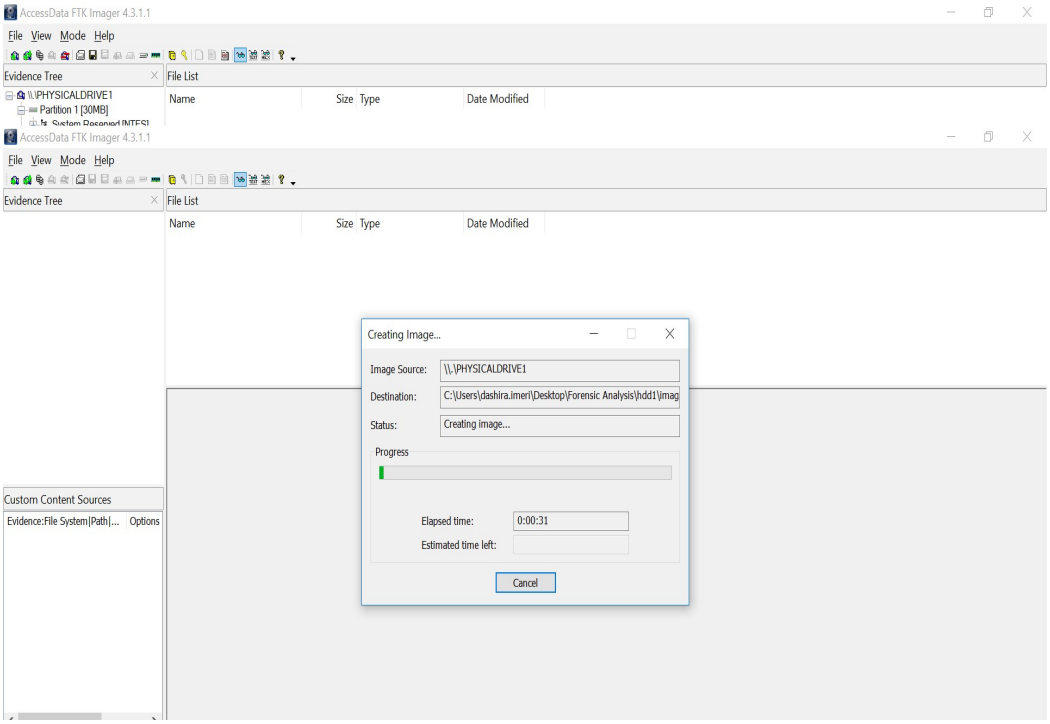


Fig. 14 Krijimi i imazhit të diskut

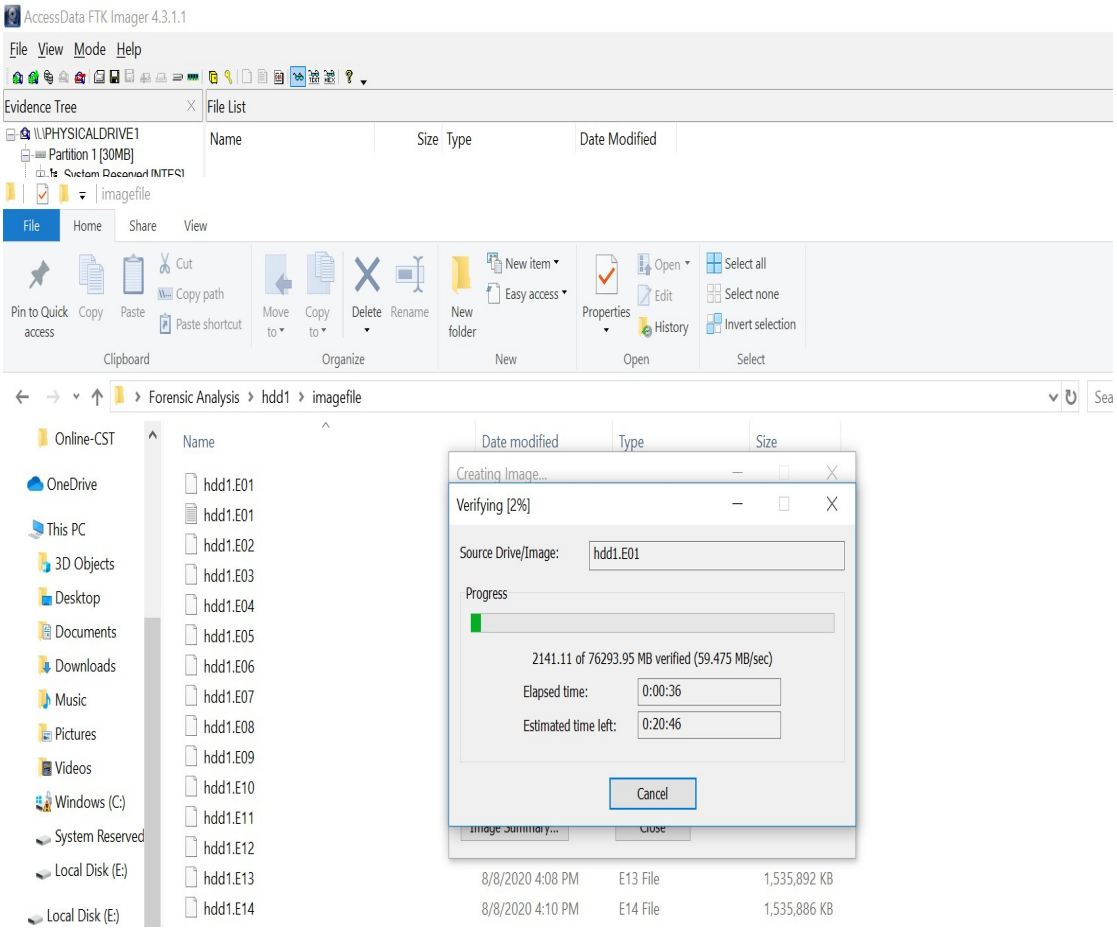


Fig.15 Verifikim i procesit të krijimit të imazhit të diskut

Pasi të ketë mbaruar verifikimi, në monitor do të na shfaqet një dritare informuese - e paraqitur në figurën 15. Shpejtësia e krijimit të imazhit forenzik ndryshon bazuar në harduerin që posedojm.

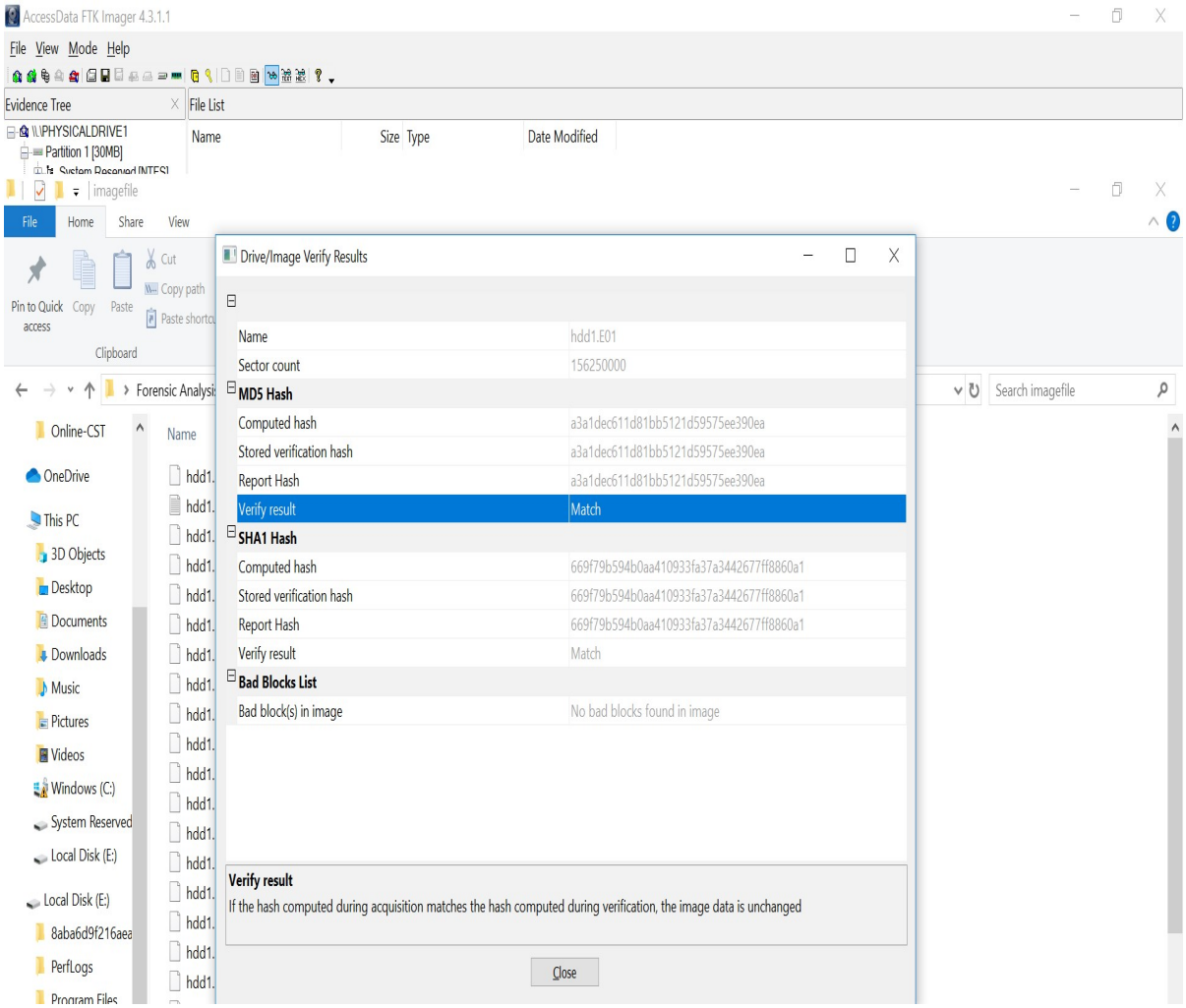


Fig. 16 Rezultati nga verifikimi i imazhit të hard-diskut 1

3.4 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 1

Raporti që u gjenerua pas verifikimit të rezultatit nga FTK imager per *hard*-diskun 1 është si në vijim:

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: 100776

Evidence Number: hdd1

Unique Description:

Examiner: Deshira Imeri

Notes: Forenzika digjitale, gjurmimi i hard- disqeve

Information for C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 9,726

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 156,250,000

[Physical Drive Information]

Drive Model: WDC WD80 0JD-75MSA3 USB Device

Drive Serial Number: WD-WMAM9SL03689

Drive Interface Type: USB

Removable drive: False

Source data size: 76293 MB

Sector count: 156250000

[Computed Hashes]

MD5 checksum: a3a1dec611d81bb5121d59575ee390ea

SHA1 checksum: 669f79b594b0aa410933fa37a3442677ff8860a1

Image Information:

Acquisition started: Sat Aug 8 15:51:32 2020

Acquisition finished: Sat Aug 8 16:26:21 2020

Segment list:

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E01

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E02

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E03

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E04

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E05

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E06

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E07

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E08

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E09

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E10

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E11

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E12

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E13

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E14

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E15

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E16

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E17

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E18

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E19

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E20

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E21

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E22

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E23

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E24

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E25

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd1\imagefile\hdd1.E26

Image Verification Results:

Verification started: Sat Aug 8 16:26:22 2020

Verification finished: Sat Aug 8 16:41:47 2020

MD5 checksum: a3a1dec611d81bb5121d59575ee390ea : verified

SHA1 checksum: 669f79b594b0aa410933fa37a3442677ff8860a1 : verified

Në këtë raport të gjeneruar mund te shohim qartë specifikacionin e *hard*-diskut për të cilin është krijuar imazh forenzik, informacionin mbi krijim e imazhit - fillimi dhe mbarimi i të njëjtit duke treguar ditën, muajin dhe vitin, si dhe periudhën kohore të fillimit dhe mbarimit të krijimit të imazhit forenzik të *hard*-diskut 1. Krijimi i të njëjtit zgjati:

Acquisition started: Sat Aug 8 15:51:32 2020

Acquisition finished: Sat Aug 8 16:26:21 2020

Në të njëtin raport gjejmë të dhëna edhe për verifikimin e imazhit të krijuar, si dhe të dhëna mbi MD5 dhe SHA1, të cilat paraqesin hash funksione kriptografike te *hard*-diskut 1:

Image Verification Results:

Verification started: Sat Aug 8 16:26:22 2020

Verification finished: Sat Aug 8 16:41:47 2020

MD5 checksum: a3a1dec611d81bb5121d59575ee390ea : verified

SHA1 checksum: 669f79b594b0aa410933fa37a3442677ff8860a1 : verified

Gjenerim i raportit për verifikim nga FTK *Imager* për *hard*-diskun 1 zgjati 34 minuta e 49 sekonda, kurse verifikimi i raportit të gjeneruar zgjati 15 minuta e 25 sekonda.

Artikulli i dëshmisë të FTK-së *(ang.FTK Evidence Item)*

Përmes opsionit 'shto artikullin e dëshmisë' (ang. *Add Evidence Item*), siç shihet në figuriën 17, fillon procesi i përzgjedhjes të burimin për krijimin e imazhit.

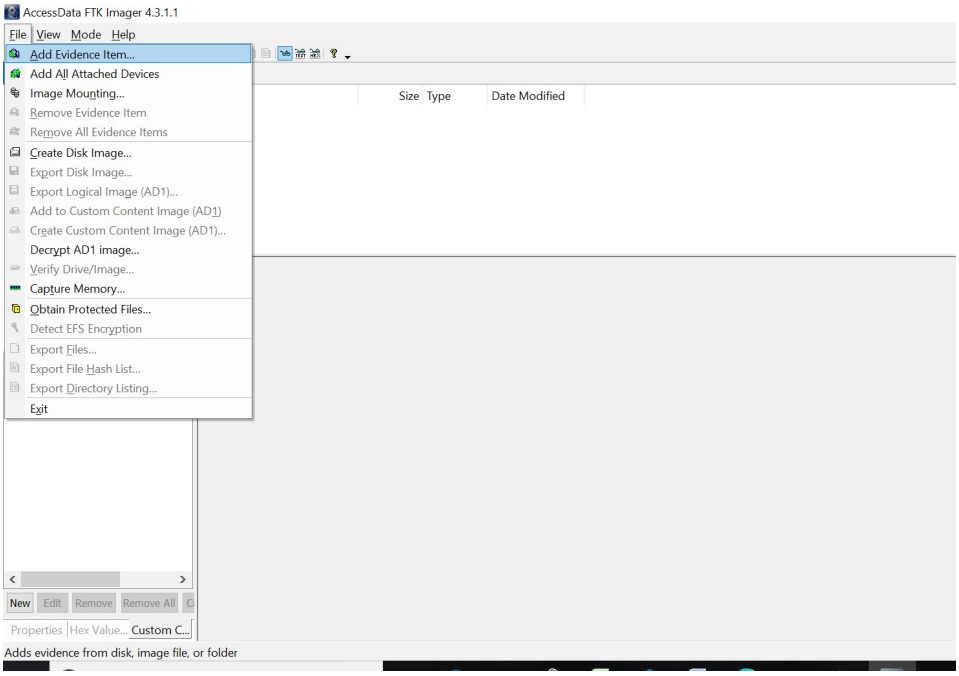


Fig. 17 Artikulli i dëshmive FTK-së

Pastaj na shfaqet dritarja komunikuese '*Select Source*' ku, për të krijuar imazhin forensik, përzgjedhim *'Physical drive'*. Të njejtën mund ta vërejmë më poshtë në figurën 18:

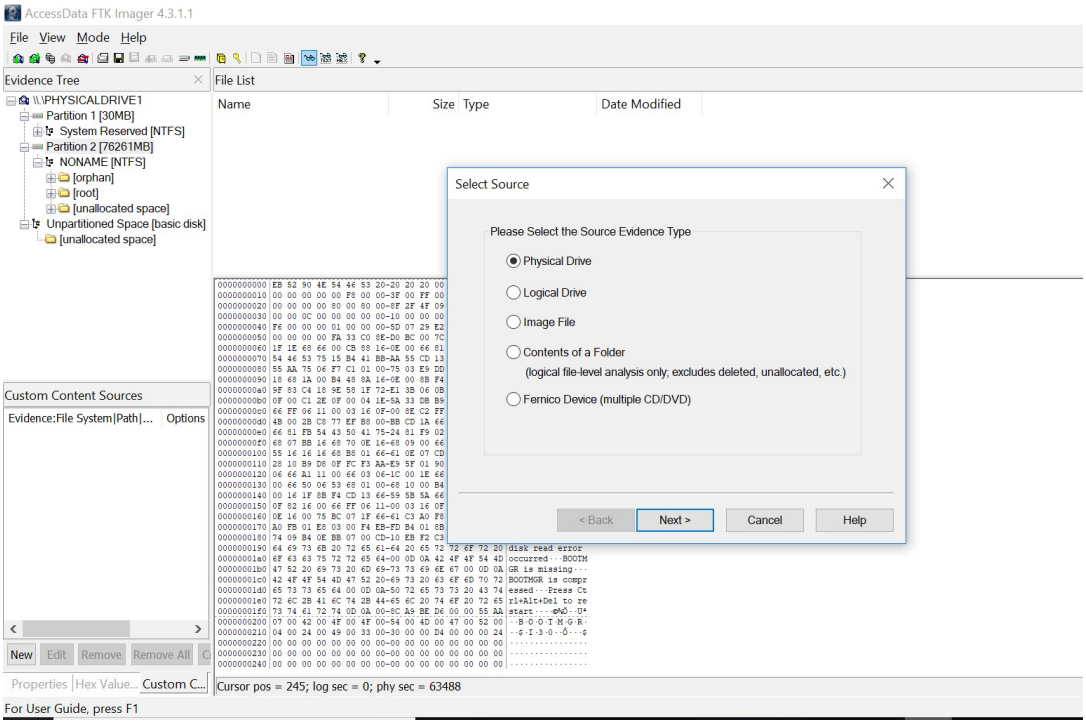


Fig. 18 Përzgjedhja e diskut fizik gjatë krijimit të imazhit për hard-diskun 1

Shtimi i FTK provave/ dëshmive duke përzgjedhur diskun fizik

(ang. *FTK add evidence items selected physical drive*)

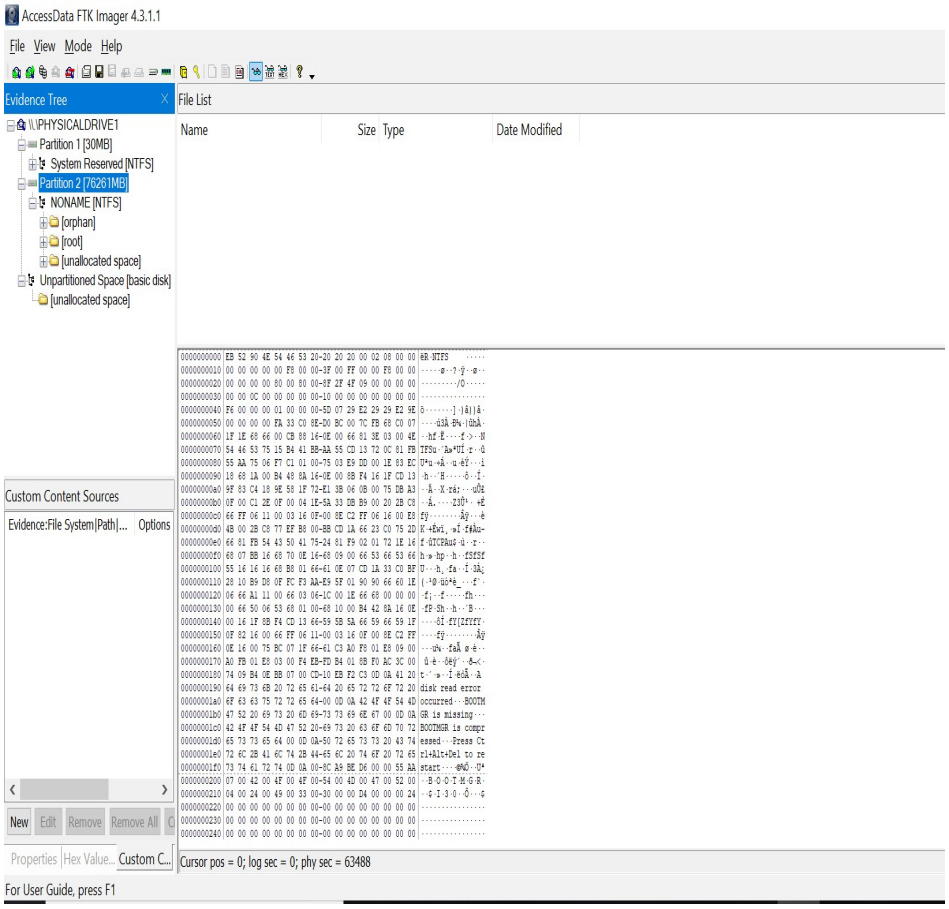


Fig. 19 Shtimi i FTK provave duke përzgjedhur diskun fizik

Shtimi i evidencës në FTK Imager duke përzgjedhur burimin (ang.*FTK add evidence select source)*

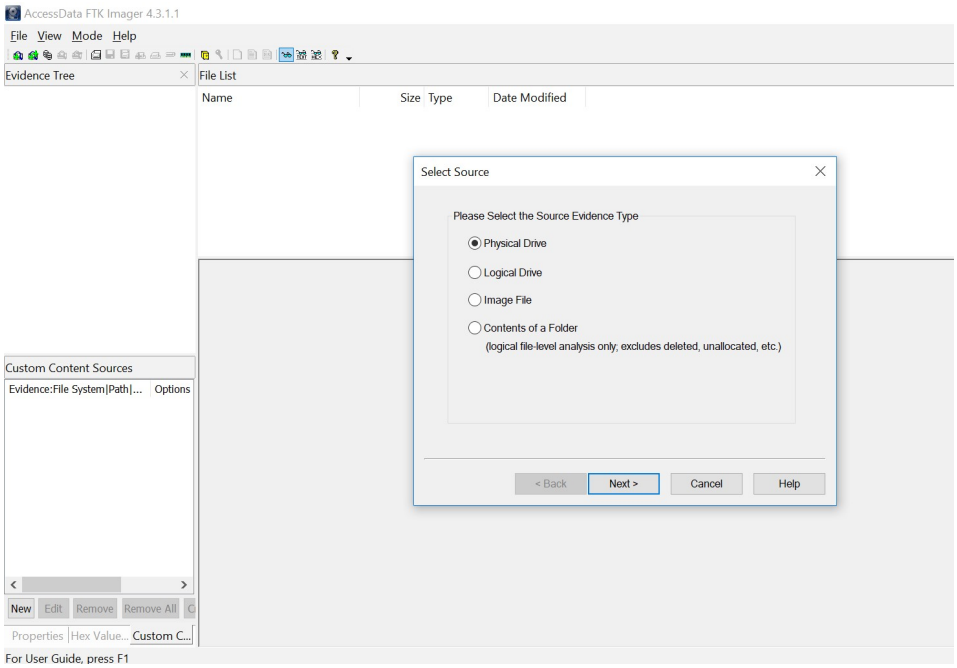


Fig. 20 Shtim i evidencës në FTK Imager duke e përzgjedhur burimin

Shtimi i evidencës në FTK Imager duke e përzgjedhur diskun fizik:

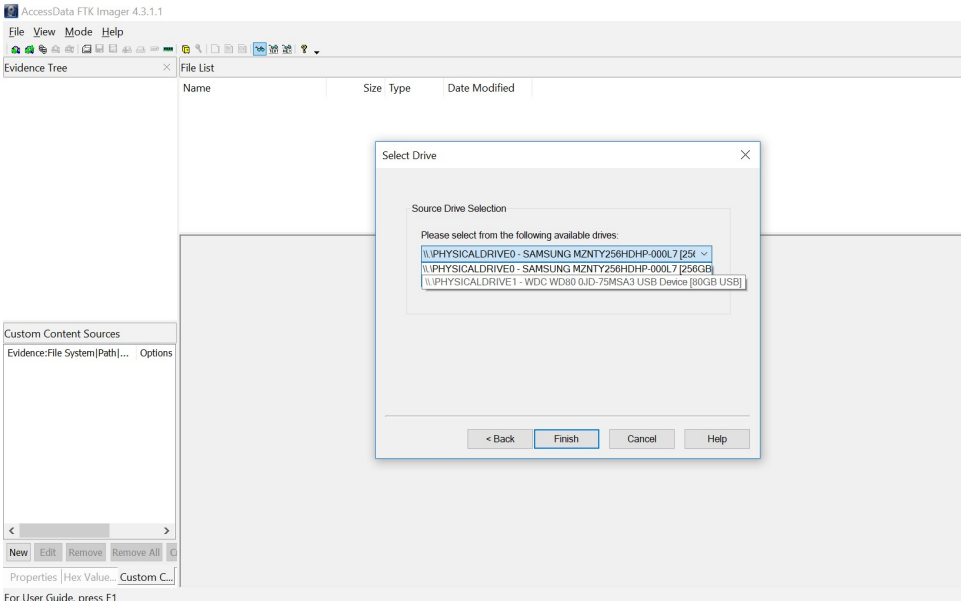


Fig. 21 Shtim i evidencës në FTK Imager duke e përzgjedhur diskun fizik

Këta etapa për krijimin e imazheve të disqeve janë përdorur edhe për tre *hard*-disqet tjera me radhë (hard-disku 2, hard- disku 3 dhe hard-diksu 4). Me qëllim që të mos përsëritemi, në vijim do të mund të gjeni rezultatet e verifikimit të imazheve për hard-disqet 2, 3 dhe 4.

3.5 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 2

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: HDD2

Evidence Number:

Unique Description:

Examiner: Deshira Imeri

Notes: Forenzika digjitale, gjurmimi i hard-disqeve

Information for C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 9,726

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 156,250,000

[Physical Drive Information]

Drive Model: WDC WD80 0JD-75MSA3 USB Device

Drive Serial Number: WD-WMAM9SP32232

Drive Interface Type: USB

Removable drive: False

Source data size: 76293 MB

Sector count: 156250000

[Computed Hashes]

MD5 checksum: 90ba990b30524ec0283db3d94b05b70d

SHA1 checksum: 3ee79a6c8bd16dae352aee863a9bef88e370c169

Image Information:

Acquisition started: Sat Aug 8 20:13:54 2020

Acquisition finished: Sat Aug 8 20:47:47 2020

Segment list:

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E01

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E02

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E03

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E04

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E05

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E06

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E07

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E08

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E09

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E10

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E11

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E12

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E13

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd2\HDD2_image\HDD2.E14

Image Verification Results:

Verification started: Sat Aug 8 20:47:47 2020

Verification finished: Sat Aug 8 20:56:53 2020

MD5 checksum: 90ba990b30524ec0283db3d94b05b70d : verified

SHA1 checksum: 3ee79a6c8bd16dae352aee863a9bef88e370c169 : verified

Prej ku mund të shihet qartë specifikacioni i *hard*-diskut për të cilin është krijuar imazhi forenzik, informacionin mbi krijim e imazhit - fillimi dhe mbarimi i të njëjtit duke treguar ditën, muajin dhe vitin, si dhe periudhën kohore të fillimit dhe mbarimit të krijimit të imazhit forenzik të *hard*-diskut 2. Krijimi i të njëjtit zgjati:

Acquisition started: Sat Aug 8 20:13:54 2020

Acquisition finished: Sat Aug 8 20:47:47 2020

Në të njëtin raport gjejmë të dhëna edhe për verifikimin e imazhit të krijuar, si dhe të dhëna mbi MD5 dhe SHA1 të cilat paraqesin hash funksione kriptografike te *hard*-diskut 2:

Image Verification Results:

Verification started: Sat Aug 8 20:47:47 2020

Verification finished: Sat Aug 8 20:56:53 2020

MD5 checksum: 90ba990b30524ec0283db3d94b05b70d : verified

SHA1 checksum: 3ee79a6c8bd16dae352aee863a9bef88e370c169 : verified

Gjenerimi i raportit për verifikim nga FTK *Imager* për *hard*-diskun 2 zgjati 33 minuta e 53 sekonda, kurse verifikimi i raportit të gjeneruar zgjati 9 minuta e 6 sekonda.

3.6 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 3

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: HDD3

Evidence Number:

Unique Description:

Examiner: Deshira Imeri

Notes: Forenzika digjitale, gjurmimi i hard- disqeve

Information for C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 9,726

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 156,250,000

[Physical Drive Information]

Drive Model: WDC WD80 0JD-75MSA3 USB Device

Drive Serial Number: WD-WMAM9SP32232

Drive Interface Type: USB

Removable drive: False

Source data size: 76293 MB

Sector count: 156250000

[Computed Hashes]

MD5 checksum: 9cbe286dc3cd4ba2f142110b7cd26e7b

SHA1 checksum: d7a37e4f2b4016600dbab23c167ceae683446f27

Image Information:

Acquisition started: Sat Aug 8 21:12:04 2020

Acquisition finished: Sat Aug 8 21:45:06 2020

Segment list:

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E01

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E02

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E03

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E04

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E05

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E06

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E07

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E08

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E09

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E10

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E11

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E12

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E13

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E14

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E15

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E16

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E17

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E18

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E19

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E20

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E21

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd3\hdd3_image\hdd3.E22

Image Verification Results:

Verification started: Sat Aug 8 21:45:07 2020

Verification finished: Sat Aug 8 21:56:10 2020

MD5 checksum: 9cbe286dc3cd4ba2f142110b7cd26e7b : verified

SHA1 checksum: d7a37e4f2b4016600dbab23c167ceae683446f27 : verified

Nga ky raport i gjeneruar mund të shohim pra specifikacionin e *hard*-diskut për të cilin është krijuar imazhi forenzik, informacionin mbi krijim e imazhit - fillimi dhe mbarimi i të njëjtit duke treguar ditën, muajin dhe vitin si dhe periudhën kohore të fillimit dhe mbarimit të krijimit të imazhit forenzik te *hard*-diskut 3. Krijimi i të njëjtit zgjati:

Image Information:

Acquisition started: Sat Aug 8 21:12:04 2020

Acquisition finished: Sat Aug 8 21:45:06 2020

Në të njëtin raport gjejmë të dhëna edhe për verifikimin e imazhit të krijuar, si dhe të dhëna mbi MD5 dhe SHA1 të cilat paraqesin hash funksione kriptografike te *hard*-diskut 3:

Image Verification Results:

Verification started: Sat Aug 8 21:45:07 2020

Verification finished: Sat Aug 8 21:56:10 2020

MD5 checksum: 9cbe286dc3cd4ba2f142110b7cd26e7b : verified

SHA1 checksum: d7a37e4f2b4016600dbab23c167ceae683446f27 : verified

Gjenerim i raportit për verifikim nga FTK *Imager* për *hard*-diskun 3 zgjati 33 minuta e 2 sekonda, kurse verifikimi i raportit zgjati 11 minuta e 3 sekonda .

3.7 Raporti i gjeneruar nga FTK *Imager* për *hard*-diskun 4

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: HDD4

Evidence Number:

Unique Description:

Examiner: Deshira Imeri

Notes: Forenzika digjitale, investigimi i hard- disqeve

Information for C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 9,726

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 156,250,000

[Physical Drive Information]

Drive Model: WDC WD80 0JD-75MSA3 USB Device

Drive Serial Number: WD-WMAM9SF02255

Drive Interface Type: USB

Removable drive: False

Source data size: 76293 MB

Sector count: 156250000

[Computed Hashes]

MD5 checksum: 4ab7aeb7029214fd68097a86b07139ca

SHA1 checksum: 7a7709f9d9b6d9e3feb33d737a1fd0cff33b1cae

Image Information:

Acquisition started: Sat Aug 8 22:15:47 2020

Acquisition finished: Sat Aug 8 22:48:47 2020

Segment list:

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E01

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E02

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E03

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E04

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E05

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E06

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E07

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E08

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E09

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E10

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E11

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E12

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E13

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E14

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E15

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E16

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E17

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E18

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E19

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E20

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E21

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E22

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E23

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E24

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E25

C:\Users\dashira.imeri\Desktop\Forensic Analysis\hdd4\HDD4_Images\HDD4.E26

Image Verification Results:

Verification started: Sat Aug 8 22:48:48 2020

Verification finished: Sat Aug 8 23:00:58 2020

MD5 checksum: 4ab7aeb7029214fd68097a86b07139ca : verified

SHA1 checksum: 7a7709f9d9b6d9e3feb33d737a1fd0cff33b1cae : verified

Prej ku mund të shihet qartë specifikacioni i *hard*-diskut për të cilin është krijuar imazhi forenzik, informacioni mbi krijim e imazhit - fillimi dhe mbarimi i të njëjtit duke treguar ditën, muajin dhe vitin si dhe periudhën kohore të fillimit dhe mbarimit të krijimit të imazhit forenzik të *hard*-diskut 4. Krijimi i të njëjtit zgjati:

Acquisition started: Sat Aug 8 22:15:47 2020

Acquisition finished: Sat Aug 8 22:48:47 2020

Në të njëtin raport gjejmë të dhëna edhe për verifikimin e imazhit të krijuar, si dhe të dhëna mbi MD5 dhe SHA1 të cilat paraqesin hash funksione kriptografike të *hard*-diskut 4:

Image Verification Results:

Verification started: Sat Aug 8 22:48:48 2020

Verification finished: Sat Aug 8 23:00:58 2020

MD5 checksum: 4ab7aeb7029214fd68097a86b07139ca : verified

SHA1 checksum: 7a7709f9d9b6d9e3feb33d737a1fd0cff33b1cae : verified

Gjenerim i raportit për verifikim nga FTK *Imager* për *hard*-diskun 4 zgjati 33 minuta, kurse verifikimi i raportit zgjati 12 minuta e 10 sekonda.

Nga të dhënat e gjeneruara prej raporteve verifikuese për *hard*-diskun 1, 2,3 dhe 4 përmes FTK Imager shihet qartë se, krahasuar me *hard*-disqet 1, 2 dhe 3, *hard*-disku 4 ka arritur të gjenerohet për kohë më të shkurtër edhe atë për 33 minuta, kurse nga të gjitha verifikimet e raporteve të gjeneruara për *hard* disqet 1, 2, 3 dhe 4 më shpejtë ka arritur të verifikohet raporti i *hard*-diskut 2 edhe atë për 9 minuta e 6 sekonda.

3.8 Montim i imazhit për *hard*-diskun 1

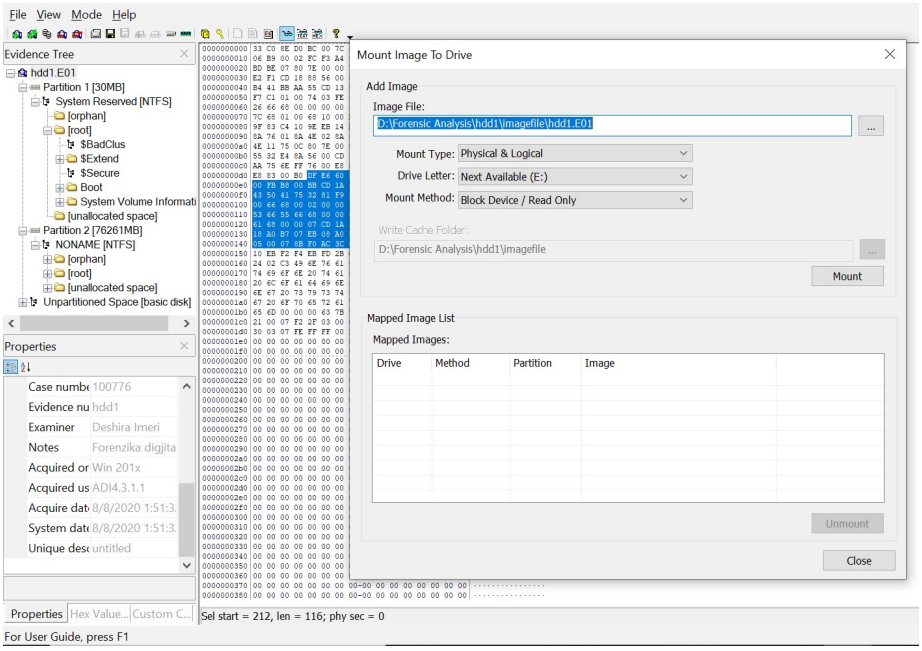


Fig. 22 Montim i imazhit (ang. *Image mountain*) për *hard*- diskun 1

Përmes montimit të imazhit *(ang. image mounting)* bëhet montimi i të gjitha imazheve të krijuara më parë në *hard*-disk. Përmes të njëjtit mund të shihet struktura e direktoriumit si dhe e të gjithë file-eve të krijuara në sistemin strukturor.

3.9 Autopsy 4.15.0

Çfarë është Autopsy?

Autopsy është një vegël e forensikës digjitale me burim të hapur përdorimi (ang. open source) e krijuar nga Basis Technology, e lëshuar për herë të parë në përdorim në vitin 2000.

Është një vegël me përdorim pa pagesë dhe mjaft efikase për gjurmimin e *hard*-disqeve me karakteristika të tilla siç janë rastet me shumë përdorues (ang. *multi-user cases*), analiza kohore, (ang. *timeline analysis*), analiza e regjistrit (ang. *registry analysis*), kërkimi i fjalëve kyçe (*keyword search*), analiza e emaileve (*email analysis),* rishikim i mediave (*media playback*), analiza EXIF (*EXIF analysis*), zbulimi i *file*-ve me qëllim të keq dhe shumë më tepër (*malicious file detection*).

Ne këtë hulumtim, për analizë të imazheve digjitale të krijuara përmes veglës digjitale forenzike FTK Imager 4.3.1.1, është përdorur platforma forenzike digjitale *Autopsy* 4.15.0. Përmes kësaj vegle për analizë të imazheve forenzike është bërë analiza e katër *hard*- disqeve si dhe krahasimi në mes tyre. Më poshtë janë analizat e bëra si dhe rezultatet e fituara nga testimet e bëra.

Analizimi i të dhënave përmes *Autopsy* përdor rrjedhën e mëposhtme të punës:

1. Krijimi i një rasti (ang. *Create a Case*)

2. Shtimi i një burimi të të dhënave (ang. *Adding a Data Source*)

3. Analiza me Modulet e Përziera (ang. *Analyze with Ingest Modules*)

4. Analiza manuale (ang. *Manual Analysis*)

5. Gjenerimi i raportit (ang. *Report Generation*) (Anon., 2012)

3.10 Analiza e imazheve digjitale të krijuara për hard-disqet 1, 2, 3 dhe 4 duke perdorur veglën forenzike digjitale Autopsy 4.15.0

Nga analiza e imazhit forenzik të *hard*-diskut 1 në platformën digjitale forenzike Autopsy 4.15.0 na u shfaqen të gjitha të dhënat të cilat i ka poseduar hard-disku 1 dhe të kategorizuara në menyrë automatike. Vetë aplikacioni e ka analizuar strukturën e folderëve dhe e ka gjeneruar pamjen si në vijim:

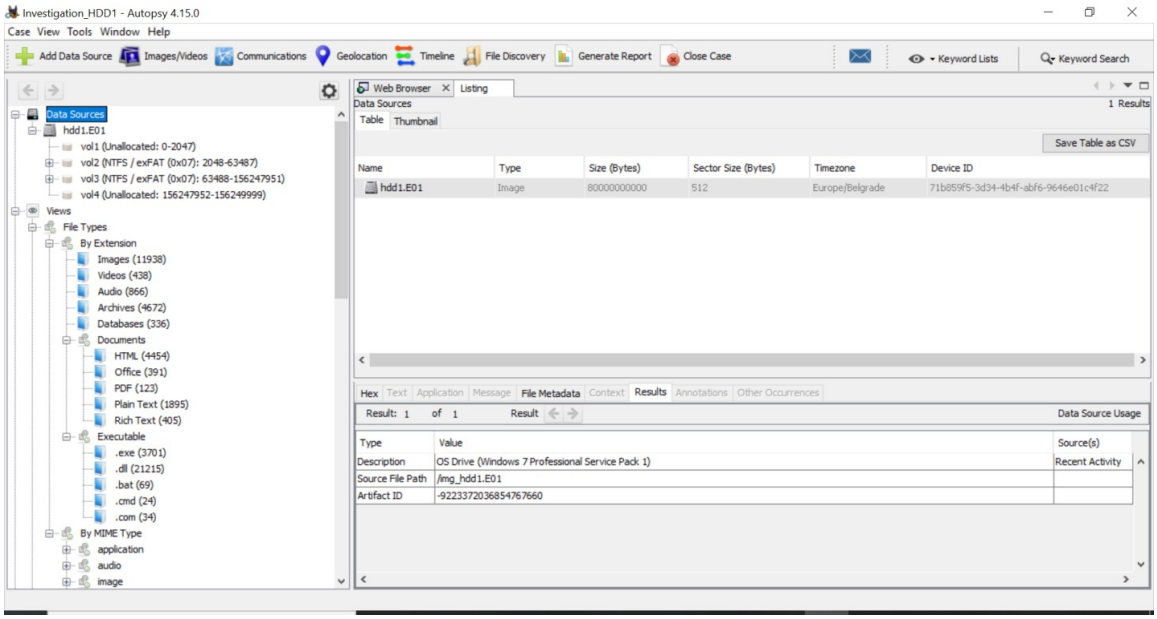


Fig. 23 Analiza e imazhit forenzik të diskut për hard-diskun 1

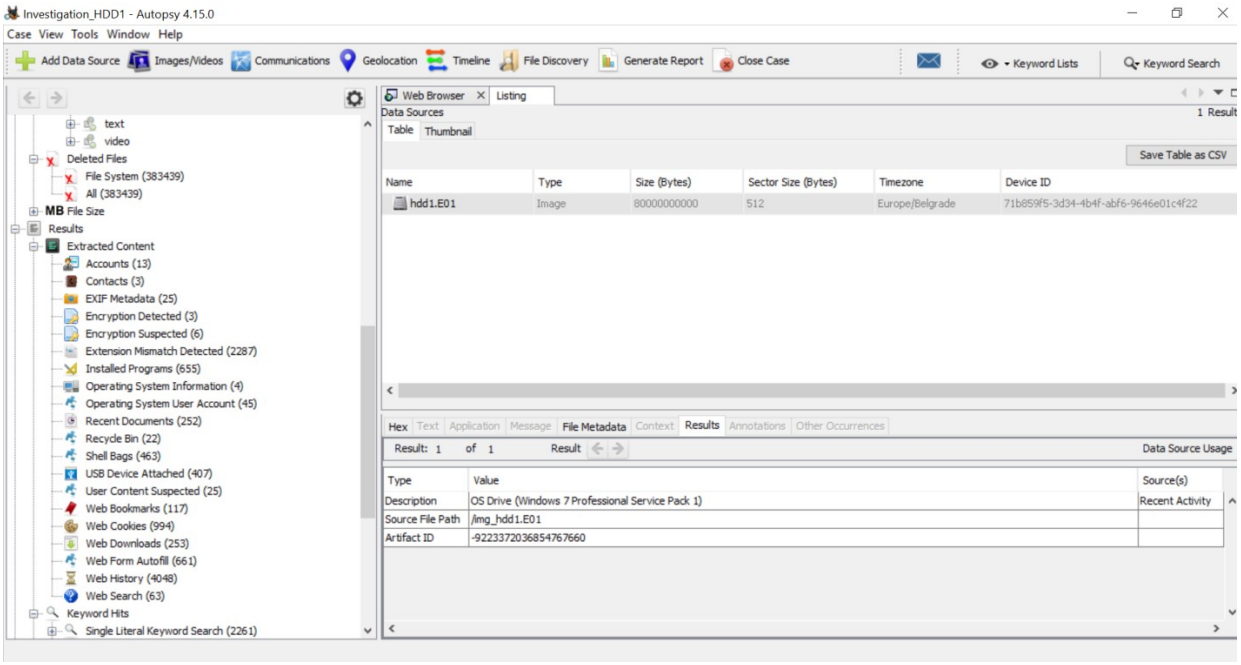


Fig. 24 Analiza e imazhit forenzik të diskut për hard-diskun 1- pjesa II

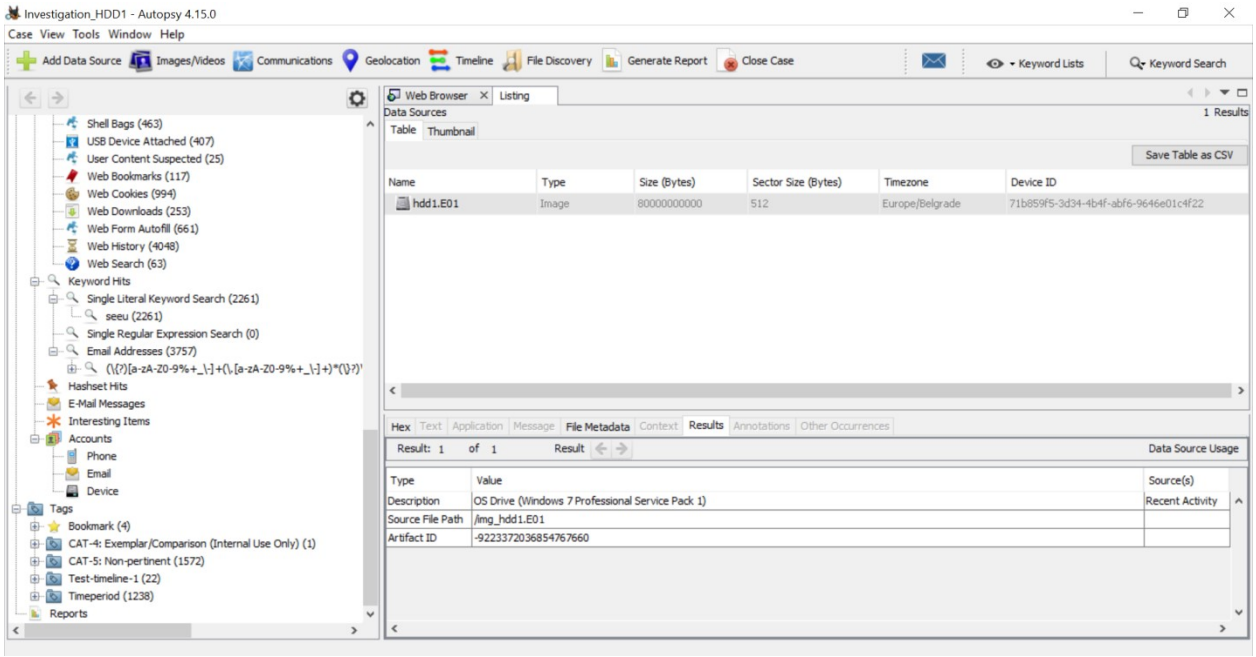


Fig. 25 Analiza e imazhit forenzik të diskut për hard-diskun 1- pjesa III

Nga figurat 23, 24 dhe 25 më lartë qartë mund të shihen pamjet e përmbajtjes së imazheve të krijuara të hard-diskut 1. Fillimisht, ajo që ne mund të verejmë, është pamja e pemës së degëzuar të imazhit të hard-diksut 1 në gjuhën angleze e njohur si *Tree Viewer*.

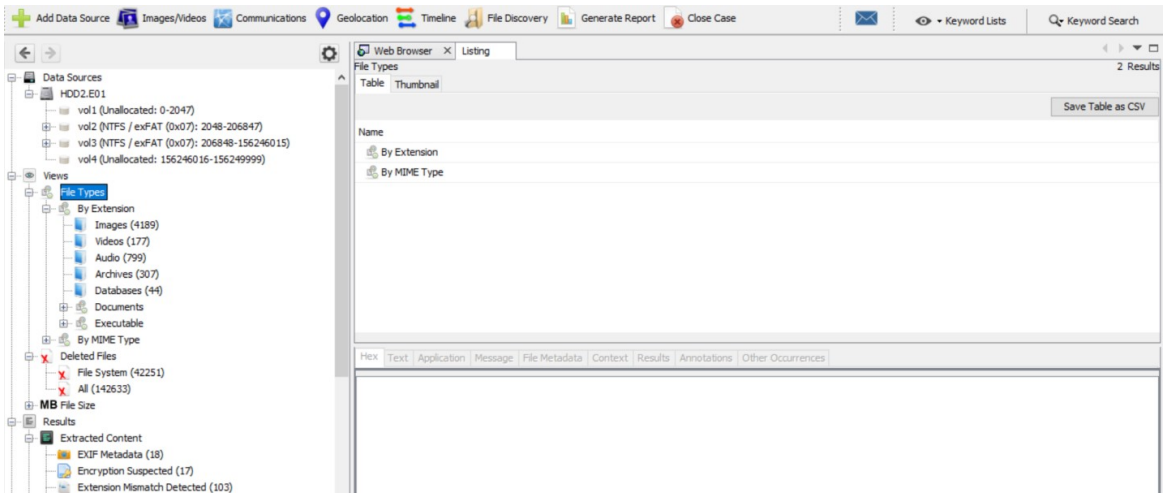


Fig. 26 Analiza e imazhit forenzik të diskut për *hard*-diskun 2- pjesa I

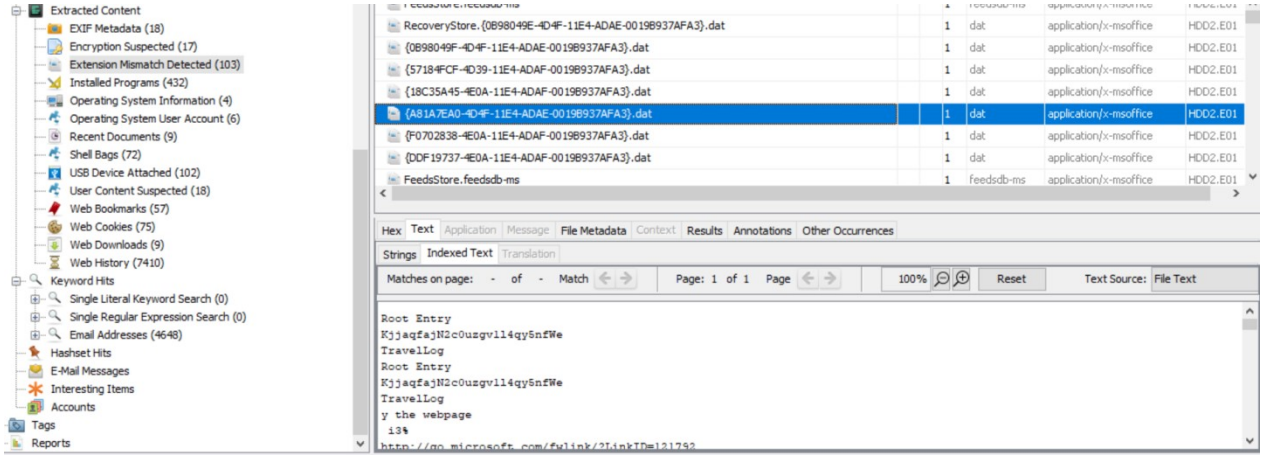


Fig. 27 Analiza e imazhit forenzik të diskut për *hard*-diskun 2- pjesa II

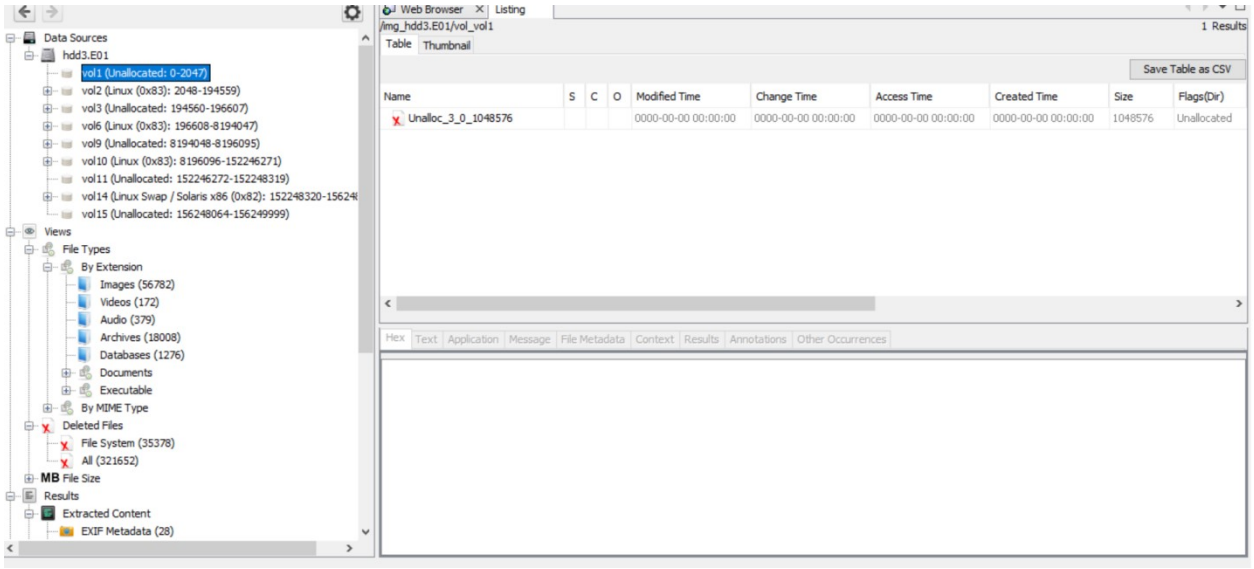


Fig. 28 Analiza e imazhit forenzik të diskut për *hard*-diskun 3- pjesa I

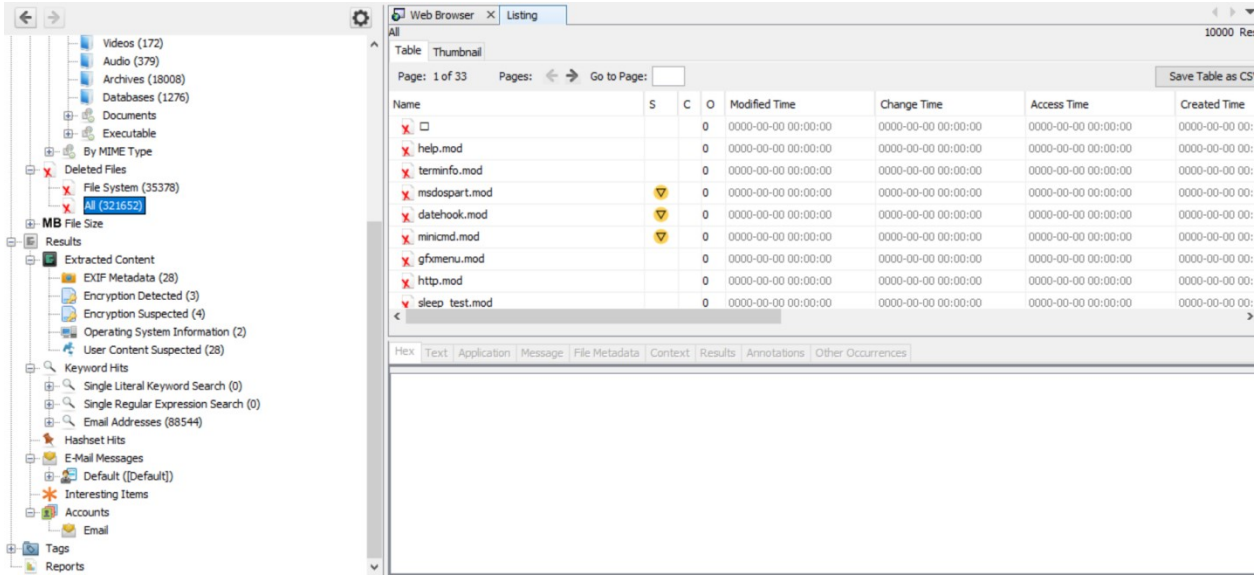


Fig. 29 Analiza e imazhit forenzik të diskut për hard-diskun 3- pjesa II

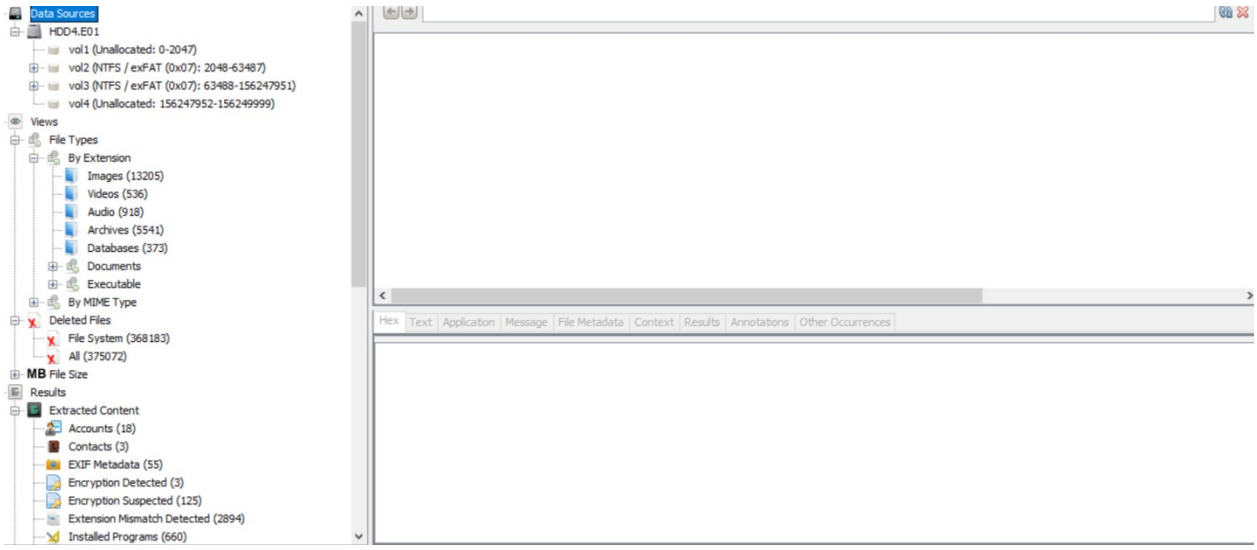


Fig. 30 Analiza e imazhit forenzik të diskut për *hard*-diskun 4- pjesa I

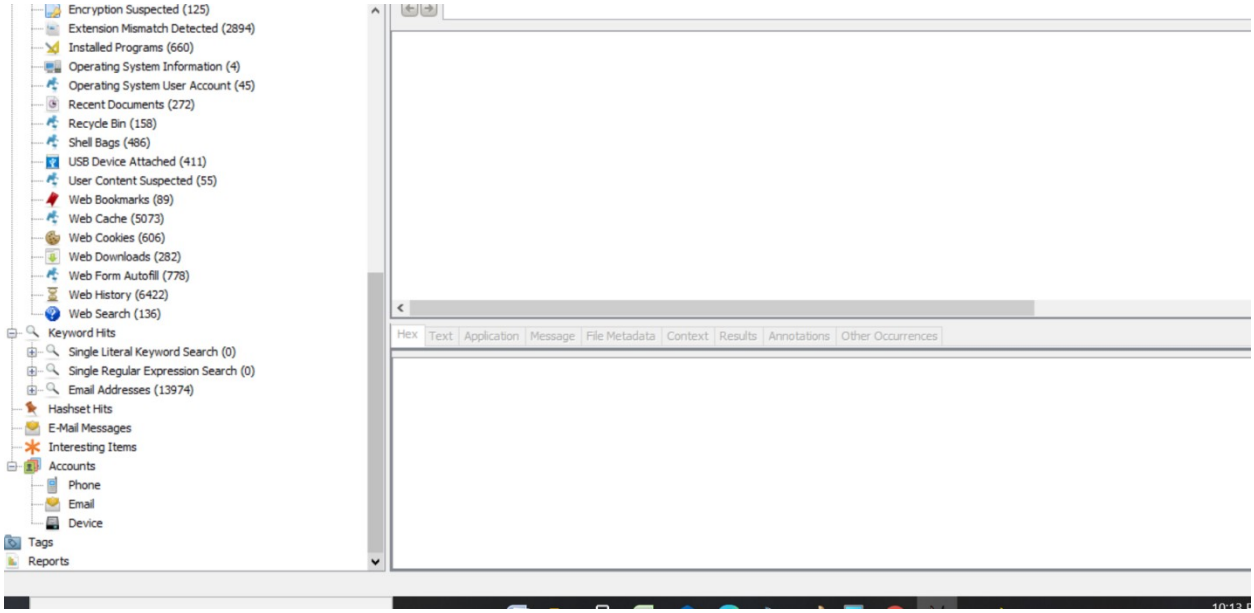


Fig. 31 Analiza e imazhit forenzik të diskut për hard-diskun 4- pjesa II

Në bazë të analizës së imazheve të disqeve për hard-disqet 1, 2, 3 dhe 4 vërehet se çdo *hard*-disk ndahet në disa partitura voluminoze në bazë të përbërjes së tyre. Për dallim nga *hard* disqet tjera *hard*-disku 3 dallon në përbërjen dhe përmbajtjen e partiturave voluminoze që posedon. Në *hard*-diskun 3 vërehen edhe partitura voluminoze me përbmajtje *Linux*.

Hapësira e pa alokuar, e referuar edhe si "hapësirë e lirë", është zona në një *hard*-disk ku mund të ruhen të dhëna të reja. Kur një përdorues ruan një *file* në një *hard* disk, ai ruhet duke

përdorur një sistem *file*-esh që gjurmon vendndodhjen fizike të direktoriumeve në hapësirën e caktuar.

3.11 Çka paraqet pamësi i pemës (ang. *Tree Viewer)*?

Pema në anën e majtë

Pema në anën e majtë të dritares kryesore është vendi ku mund të shihni file-et nga burimi i të dhënave (data sources) - në këtë rast hard-disku 1 dhe të gjeni rezultatet e ruajtura nga analizat e automatizuara (Ingest). Pema ka pesë zona kryesore:

Burimet e të Dhënave (ang. *Data Sources*): Kjo tregon hierarkinë e pemës së direktoriumeve të burimeve të të dhënave. Ju mund të gjurmoni në një *file* ose direktorium të veçantë këtu. Çdo burim i të dhënave, i shtuar në këtë rast, përfaqëson një nën-pemë të veçantë. Nëse shtoni një burim të dhënash shumë herë, ai do të shfaqet shumë herë.

Pamjet (ang.Views): Llojet specifike të *file*-eve nga data sources tregohen këtu, të grumbulluara sipas llojit ose vetive të tjera. *File*-et këtu mund të vijnë nga më shumë se një burim i të dhënave.

Rezultatet (ang.Results): Këtu tregohen rezultatet si nga analiza e automatizuar (marrja) që funksionon në sfond, ashtu edhe nga rezultatet e kërkimit.

Tag-et (Tags): Këtu tregohen *file*-et dhe rezultatet që janë *taguar*.

Raportet (ang. Reports): Raportet që kemi gjenerua,r ose që janë krijuar nga modulet e marrjes (ingest modules), shfaqen këtu.

Mund të përdoret gjithashtu opsioni "Group by data source", i disponueshëm përmes *View Options,* për të lëvizur nyjet e pemës Views, Results, dhe Tags nën *data source*-in përkatës. Kjo mund të jetë e dobishme për një numër të madh të rasteve për të zvogëluar madhësinë e secilës nën-pemë. (Anon., 2012)

Nga figura 32 qartë mund të shohim se fillimi i strukturimit të analizës së imazhit të hard-diksut 1 fillon përmes nyjes *Data Sources,* ku gjendet nën nyja hdd1.E01. *Data source*-i hdd1.E01 paraqet *hard*- diskun 1 i cili është i ndarë në katër volume edhe atë: volumi i parë **vol1**(ku gjendet folderi virtual i titulluar *Unallocated:*0-2047), volumi i dytë **vol2** (i cili na tregon llojin e *file* sistemit që përmban *hard*-disku NTFS/exFAT (0x07): 2048-63487), volumi i tretë **vol3**

(NTFS/exFAT (0x07): 63488-156247951) si dhe volumi i katërt **vol4** (Unallocated 156247952-156249999).

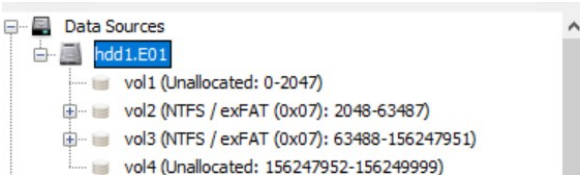


Fig. 32 Katër volumet e hard-diskut 1

Degëzimi i pemës më tej vazhdon me nyjen ***Views*** ku mund të gjejmë file-et e kategorizuara në bazë të llojit apo vetive të tjera edhe atë në: ***File Types, Deleted Files*** dhe ***MB File Size.***

Në figurën 33 shohim kategorizimin e *File Types*-it ku të gjitha *file*-et që posedon *hard*-disku 1 i ka kategorizuar në bazë të *ekstensionit* (*By Extensions*) ku marrin pjesë *file*-et me përmbajtje foto (11938), video (438), audio (866), arkivet (4672) dhe *databaza* (336). Në kategorinë dokumente (Documents) marrin pjesë *file*-et që kanë përmbajtje: HTML (4454), Office (391), PDF (123), Plain text (1895) dhe Rich Text (405). Në kategorinë *Executable* marrin pjesë *file*-t e kategorizuara në *Exe* (3701), *dll (21215), bat (69), cmd (24) dhe com (34).*

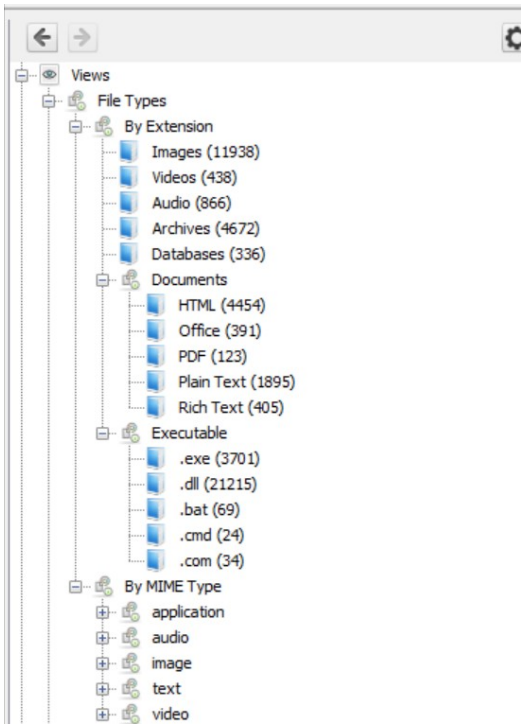


Fig. 33 Kategorizimi i *File Type*-it për hard-diskun 1

Ne llojin medial të *file*-ve të njohur si MIME *Type* (Multipurpose Internet Mail Extensions) janë kategorizuar të gjitha *file*-et e kategorisë aplikacione (application), audio, imazhe (image), tekst (text) dhe video.

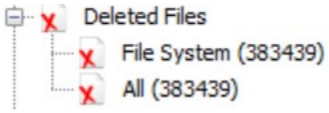


Fig. 34 *File*-at e fshirë në hard-diskun 1

Në figurën 34 mund të vërrejmë qartë nën degëzimin *file*-et e fshira (ang. *deleted files*), si rezultat i analizës së imazhit të krijuar nga hard-disku 1. Në këtë *hard*-disk gjithësejt janë 383439 *file* të fshira.

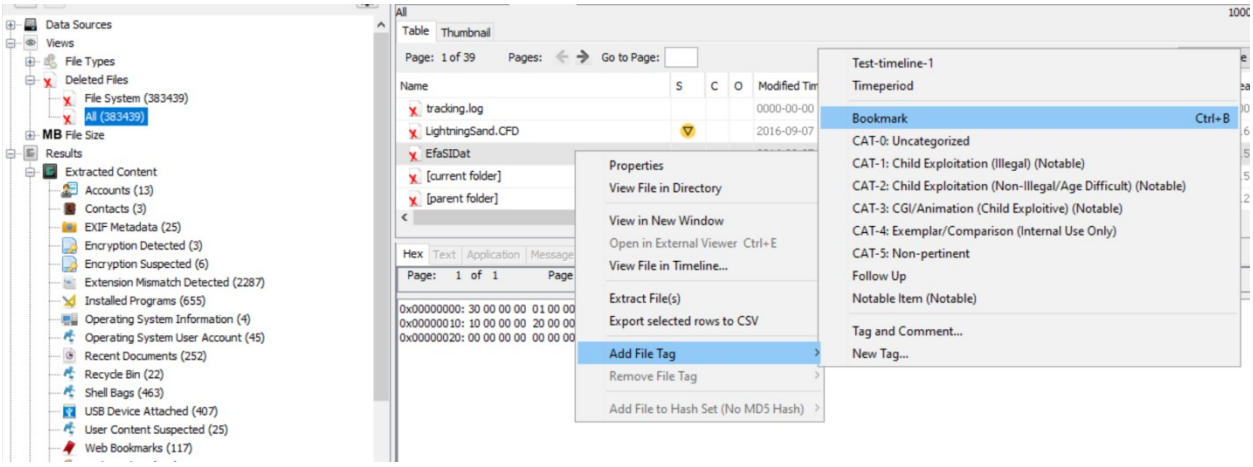


Fig. 35 *Tag*-im i *file*-ve të fshirë

Ne figurën 35 mund të vërejmë se si *file*-et e fshira mund ti *tag*-ojmë duke klikuar në *file*-in e fshirë me ndihmën e tastit të djathtë të *mous*-it duke përzgjedhur opcionin *Add File Tag* dhe më pastaj *Bookmark.* Pas kësaj procedure *file*-et që i *tag*-ojmë mund ti gjejmë në degëzimin *Tags*, të paraqitur në figurën e më poshtme:

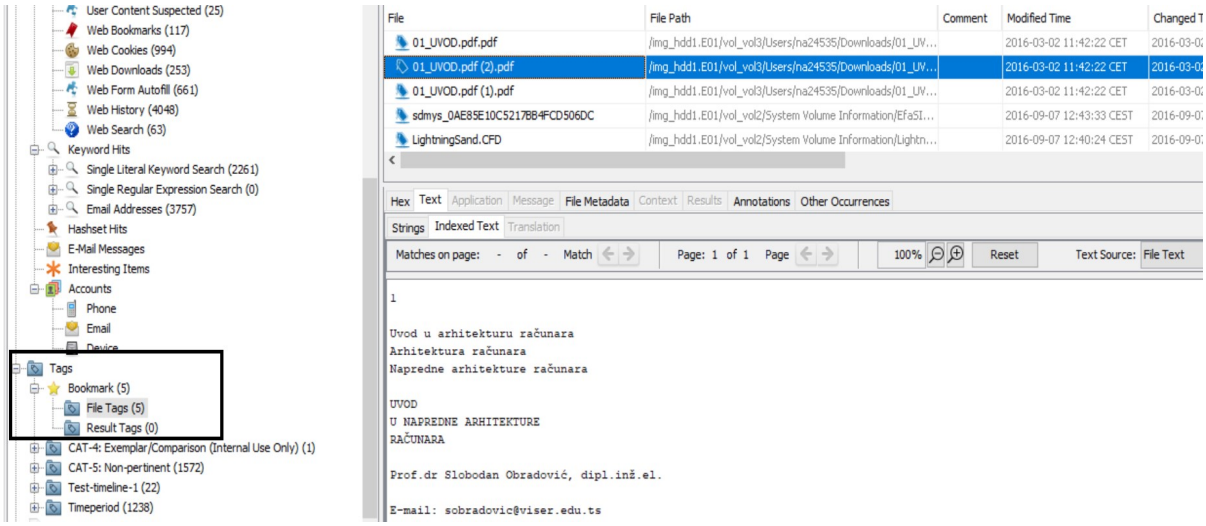


Fig. 36 *File-et* e fshira pas *tag*-imit mund ti gjejmë në *File Tags*

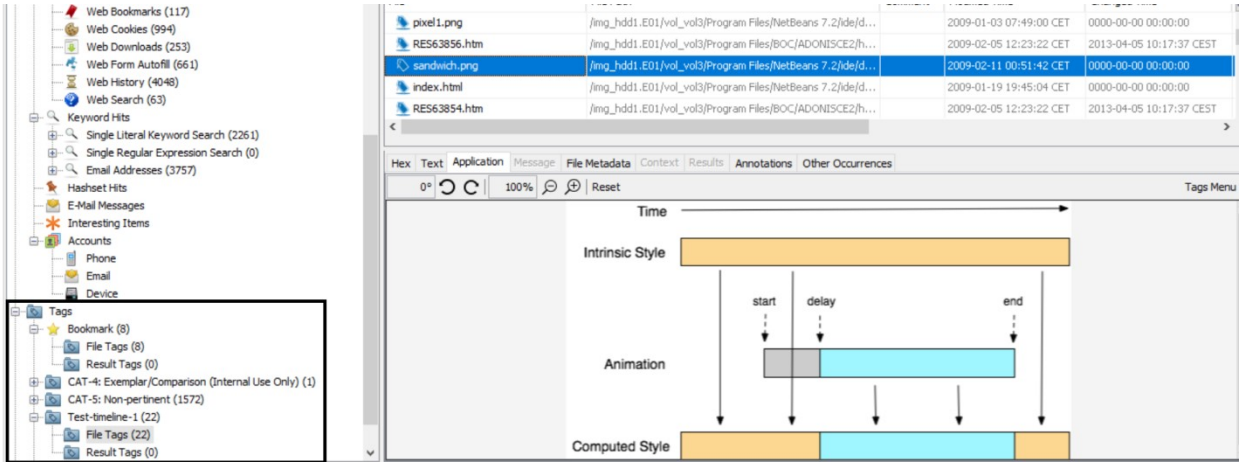


Fig. 37 *File*-et e fshira pas *tag*-imit të zgjedhur ne një *tag list* të krijuar nga ne

Me lartë vërehet se si *file*-et e fshira mund ti *tag*-ojm në një tag të ri, të krijuar dhe emëruar sipas dëshirës tonë.

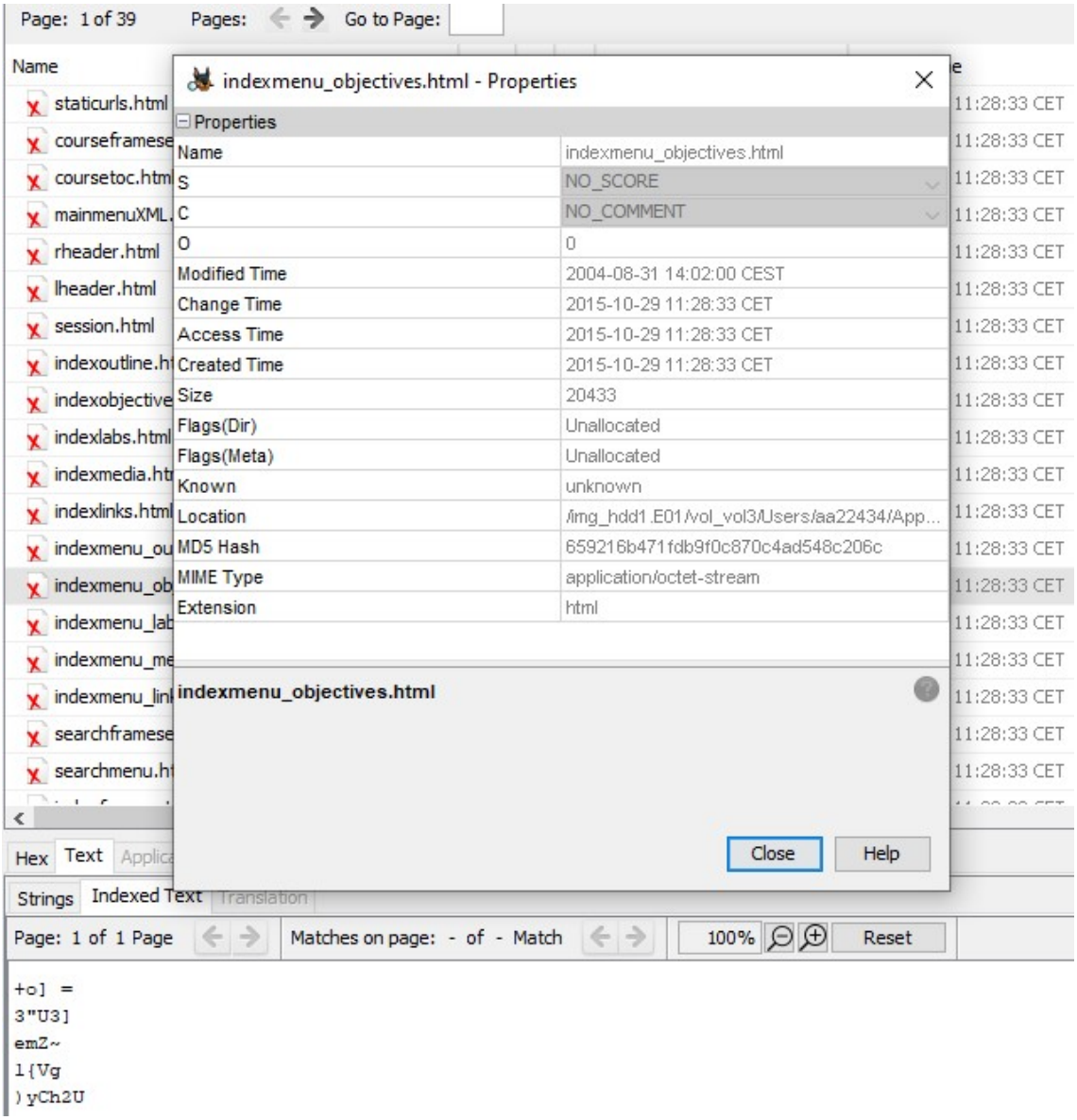


Fig. 38 Karakteristikat e *file*-it të fshirë

Nga figura 38 mund të shohim se si duket dritarja e cila tregon karakteristikat e *file*-it të fshirë, kur është krijuar, koha e modifikimit të fundit, kur i është qasur së fundmi këtij *file*-i, madhësia *e file*-it, lokacioni, *hash* vlera e MD5, lloji MIME-së, lloji i *file*-it etj. Cilësia e *file*-it të fshirë është shumë e lartë.

Në nëndegëzimin *MB File Size* janë kategorizuar të gjitha *file*-et sipas madhësisë duke u kategorizuar të gjitha edhe atë në tre kategori: 50-200 MB(75 *file*); 200 MB- 1GB (34 *file*); 1GB+(46 *file*).

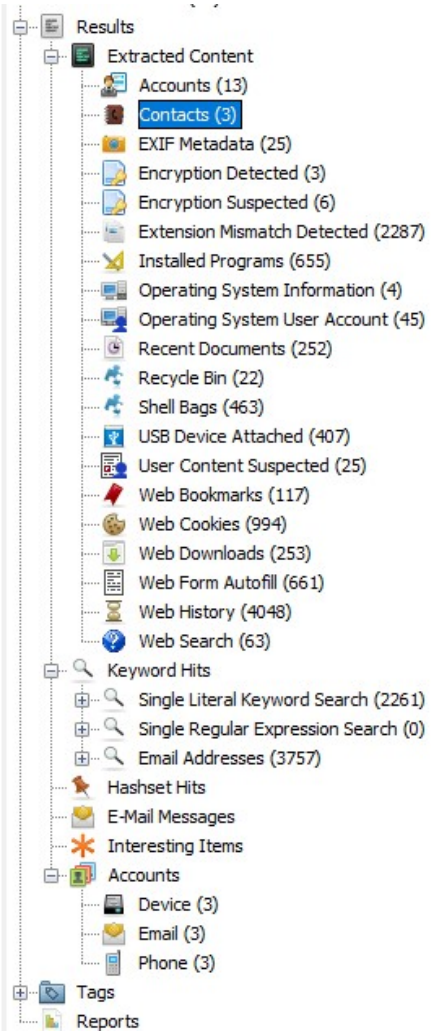


Fig. 39 Rezultatet e Hard- Diskut 1

Në degëzimin e rezultateve (ang. *results*) shihet qartë analiza e *hard*-diskut 1, prej ku mund të vërejmë detaje në lidhje me shfryëzimin e kompjuterit ku ka qenë i vendosur *hard*-disku 1. Në bazë të analizës rezulton që kompjuterin ku ka qenë i vendosur *hard*-disku 1 e kanë shfrytzuar 45 llogari të përdoruesve (user *accounts*), janë instaluar 655 programe, janë detekruar diku 407 USB piasje të bashkangjitura, *web bookmarks 117, web cookies 994, web downloads 253, web history 4048,* ndërsa janë evidentuar 3757 email adresa. Ajo që mund të vërejmë nga rezultatet e hard-diskut 1 (ang. *Results*) janë gjithashtu numrat e telefonëve që kanë qenë të bashkangjitur përmes USB porteve në këtë kompjuter.

3.12 Përmbledhje e burimit të të dhënave për *hard*-disqet 1, 2, 3 dhe *hard*- diskut 4

(ang. *Data Sources Summary for hard- drives 1, 2, 3 and hard-drive 4*)

Përmbledhje e burimit të të dhënave të një hard-disku paraqet kategorizmin e *file*-ve në kategori të caktuara siç janë kategoritë imazhe (ang. *images*), video (ang. *videos*), audio (ang. *audio*), dokume-nte (ang. *documents*), të ekzekutueshme (ang. *executables*), të panjohura (ang. *unkown*) dhe të tjera (ang. *others*). Në vijim gjejmë figurat 40, 41, 42 dhe figurën 43 të cilat paraqesin grafikonet e përmbledhjes së burimit të të dhënave për hard-disqet 1, 2, 3 dhe 4.

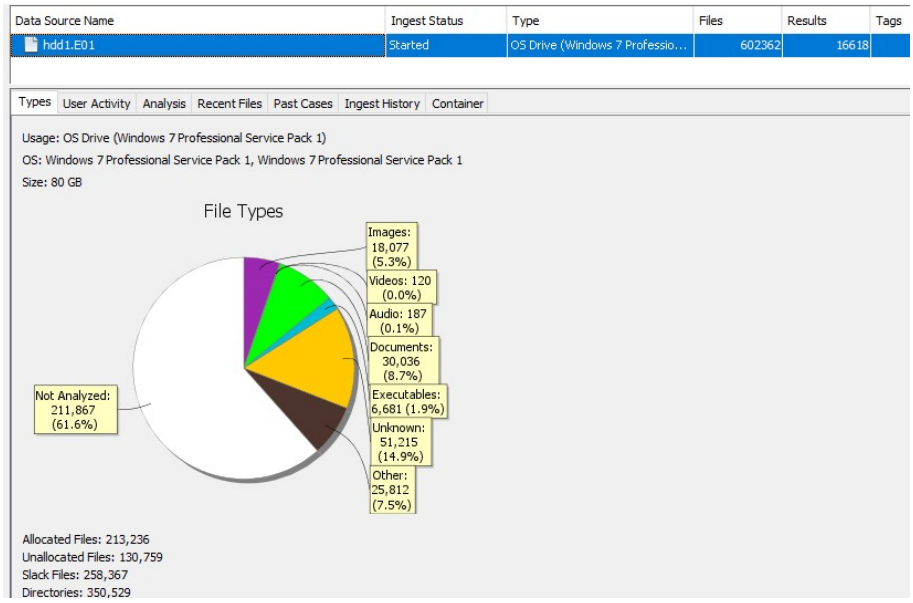


Fig. 40 Përmbledhje e burimit të të dhënave për hard-diskun 1 (ang. *Data sources summary of Hard-drive 1*)

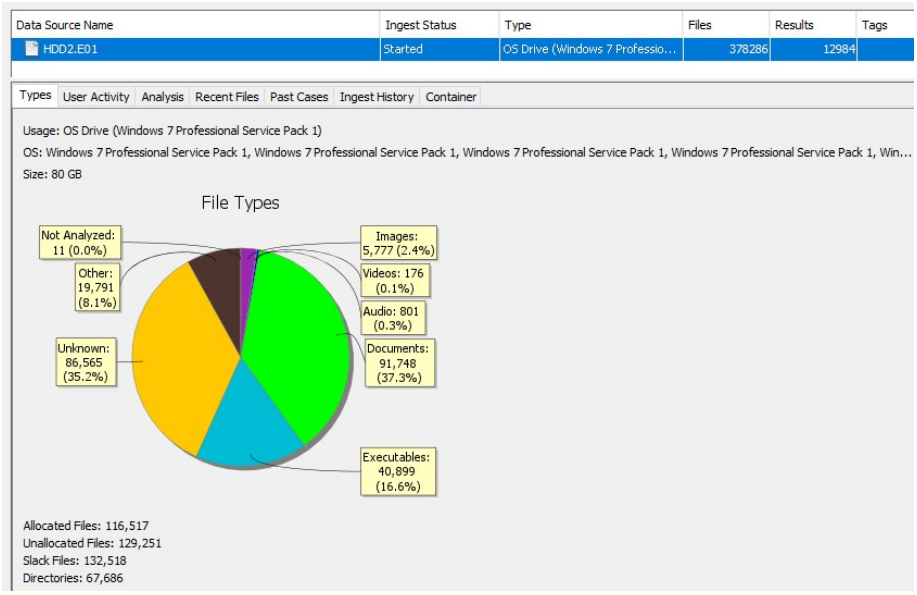


Fig. 41 Përmbledhje e burimit të të dhënave për hard-diskun 2 (ang. *Data sources summary of Hard-drive 2*)

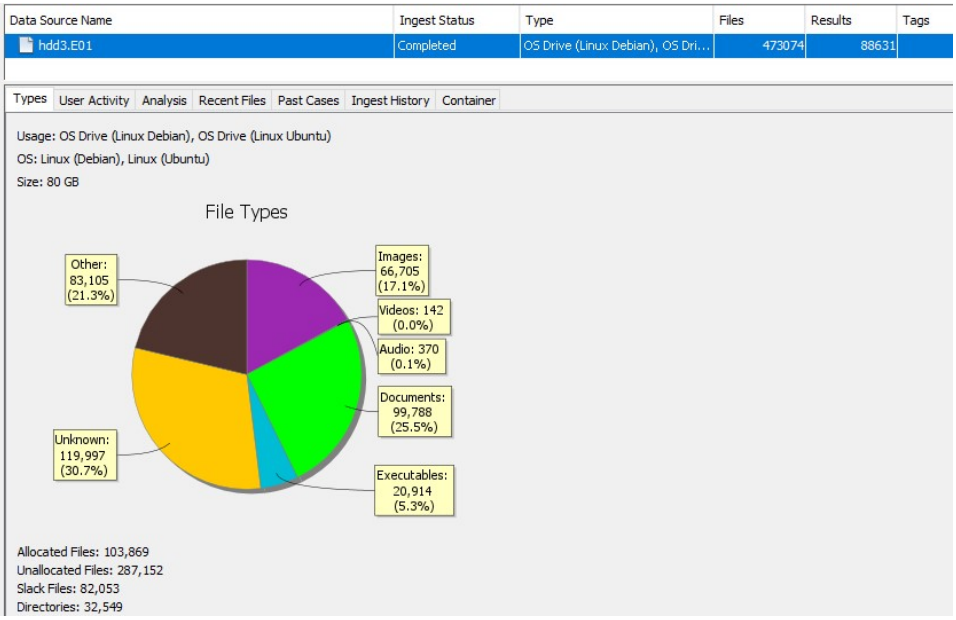


Fig. 42 Përmbledhje e burimit të të dhënave për hard-diskun 3 (ang. *Data sources summary of Hard-drive 3*)

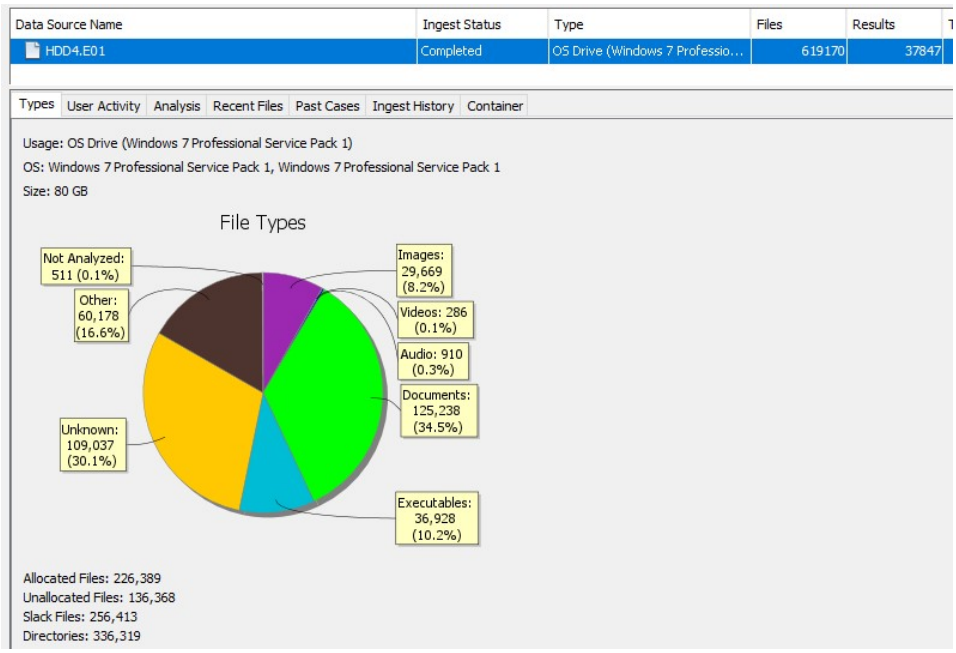
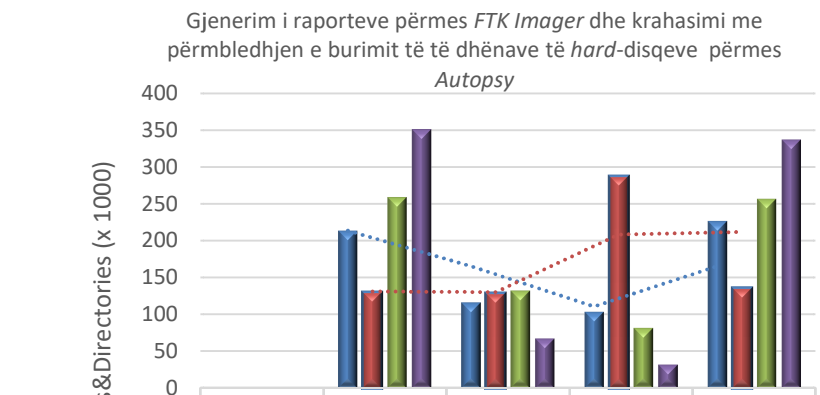


Fig. 43 Përmbledhje e burimit të të dhënave për hard-diskun 4 (ang. *Data sources summary of Hard-drive 4)*

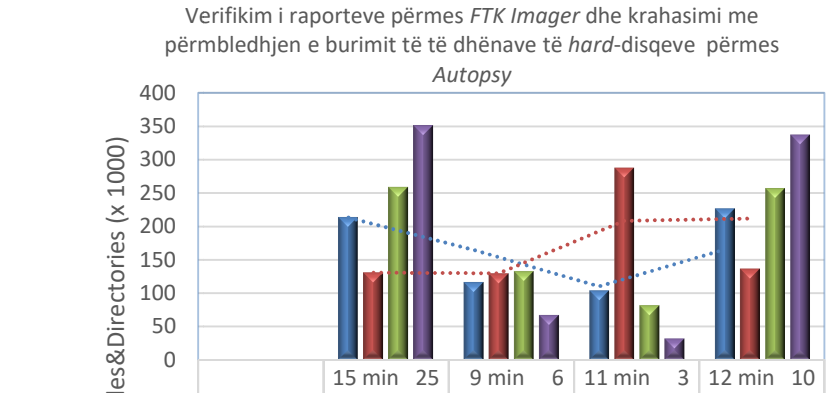
Nga Fig. ***40***40, 41**Fig. *41***, 42**Fig. *42***Fig. ***43***43 mund të vërejmë që *hard*-disku 3 ka më së shumti hapsirë të lirë (ang.*unallocated*) edhe atë 287 152 . Në bazë të përmbledhjeve të burimit të të dhënave për *hard*-disqet 1, 2, 3 dhe 4 rezulton që më së shumti file të pa analizuara në total ka *Hard*-disku 1, 61.6% ose 211 867 *file*.

HDD	Gjenerimi i raportit permes FTK Imager	Verifikimi i raportit përmes FTK Imager	Allocated files	Unallocated files	Slack Files	Directories
HDD 1	34 min 49 s	15 min 25 s	213236	130759	258367	350529
HDD 2	33 min 53 s	9 min 6 s	116517	129251	132518	67689
HDD 3	33 min 2 s	11 min 3s	103869	287152	82053	32549
HDD 4	33 min	12 min 10 s	226389	136368	256413	336319



	34' 49"s HDD 1	33' 53" HDD 2	33' 2" HDD 3	33' HDD 4
Allocated files	213236	116517	103869	226389
Unallocated files	130759	129251	287152	136368
Slack Files	258367	132518	82053	256413
Directories	350529	67689	32549	336319

Fig. 44 Gjenerim i rapoteve për *hard*-disqet 1, 2, 3 dhe 4 krahasuar me përmbledhjen e burimit të të dhënave për *hard*-disqet 1, 2, 3 dhe 4



	15 min 25 s HDD 1	9 min 6 s HDD 2	11 min 3 s HDD 3	12 min 10 s HDD 4
Allocated files	213236	116517	103869	226389
Unallocated files	130759	129251	287152	136368
Slack Files	258367	132518	82053	256413
Directories	350529	67689	32549	336319

Fig. 45 Verifikim i raporteve per *hard*-disqet 1, 2, 3 dhe 4 krahasuar me përmbledhjen e burimit të të dhënave për *hard*-disqet 1, 2, 3 dhe 4

Nëse bëjmë një krahasim të përmbledhjeve të burimit të të dhënave përmes softuerit *Autopsy* për hard-disqet 1, 2, 3 dhe 4 si dhe raporteve të gjeneruara përmes *FTK Imager* për hard-disqet 1,2,3 dhe 4, mund të konkludojmë që edhe pse *hard*-disku 4 ka më së shumti *file* të allokuara (226 389), raporti i gjenerimit të *hard*-diskut 4 përmes FTK Imager është gjeneruar për periudhë kohore më të shkurtër (33 min), krahasuar me raportet e gjeneruara përmes *FTK Imager* për *hard*-disqet 1,2 dhe 3. *Hard*-disku 1 ka më së shumti *file* të pa analizuara (211 867) 61.6%, kurse gjenerimi i raportit përmes *FTK Imager* është realizuar për periudhë kohore më të gjatë (34 min 49s) krahasuar me hard-disqet 2,3 dhe 4.

Në bazë të kësaj analize numri i *file*-ve të allokuar në një imazh forenzik nuk luan rol në kohëzgjatjen e gjenerimit të raporteve gjatë krijimit të imazheve forenzike përmas FTK *Imager*.

Për dallim të *file*-ve të allokuar, *file*-et e pa analizuara në një imazh forenzik janë në proporcion të drejtë me kohëzgjatjen e gjenerimit të raporteve për imazhet forenzike përmes FTK *Imager.*

3.13 Moduli i galerisë së imazheve dhe videove për hard-diskun 1
(ang. Images/videos gallery)

Më poshtë mund të shihet përdorimi i funksionit të galerisë së imazheve *(Images/videos)* përmes platformës *Autopsy* .

Tipari i galerisë së imazheve është krijuar në veçanti duke pasur parasysh rastet e shfrytëzimit të fëmijëve, por mund të përdoret për një larmi të llojeve të tjera të hetimit që përfshijnë imazhe dhe video. Ajo ofron veçoritë e mëposhtme përtej listës së gjatë tradicionale të miniaturave që platforma *Autopsy* dhe mjetet e tjera që ofrojnë aktualisht (Anon., 2012).

Grupon imazhet sipas dosjes (dhe atributet e tjera) për të ndihmuar ekzaminuesin të ndajë grupin e madh të imazheve në grupe më të vogla dhe për të ndihmuar të përqendrohet në zona me imazhe me interes.

Lejon ekzaminuesin të fillojë të shikojë imazhe menjëherë pas shtimit të tyre në lëndë. Derisa imazhet *hash*-ohen, ato azhurohen në *interface*. Nuk është e nevojshme të pritet derisa të merret i gjithë imazhi.

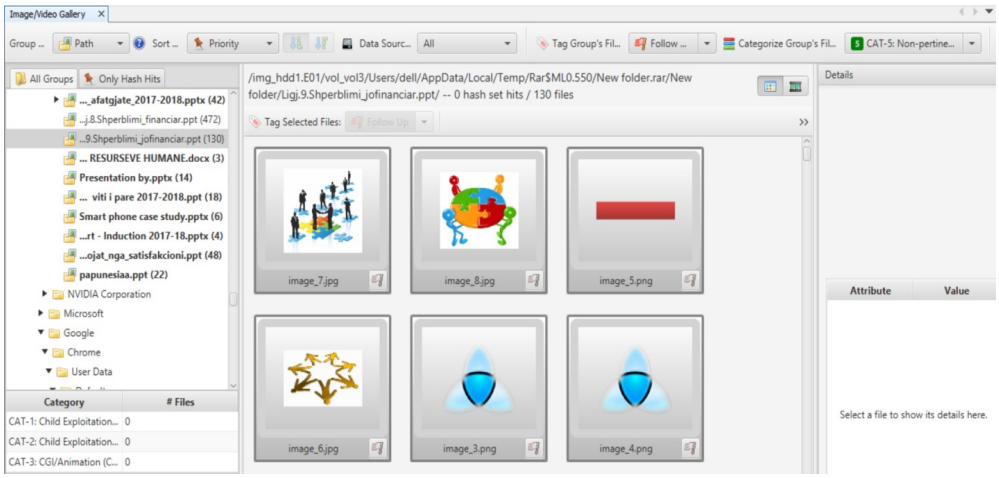


Fig. 46 Galeria e imazheve dhe videove në *hard*-diskun 1

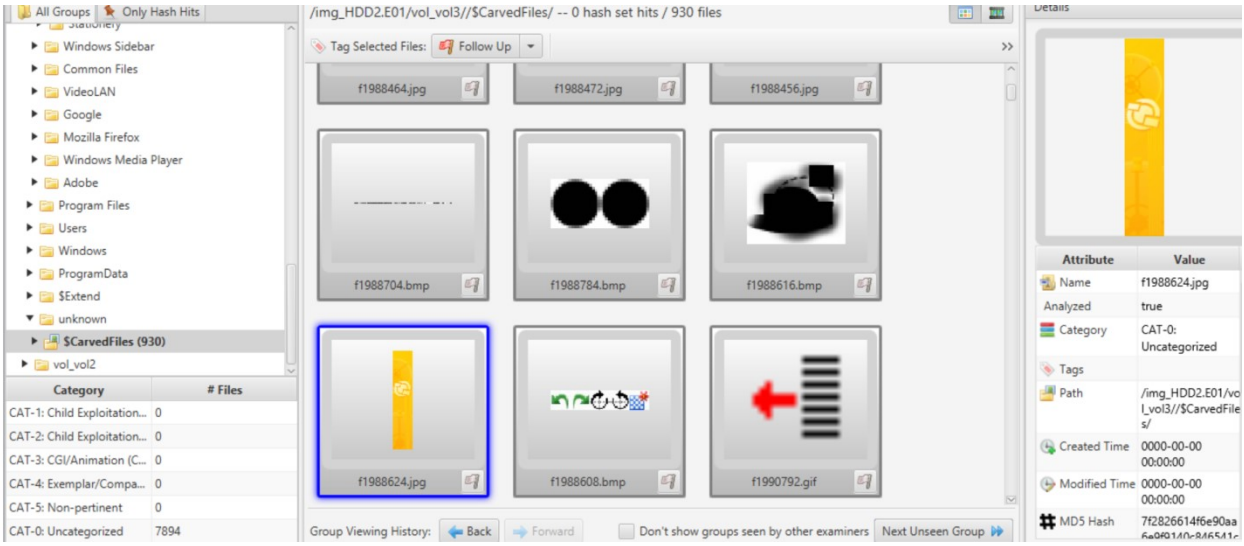


Fig. 47 Galeria e imazheve dhe videove në *hard*-diskun 2

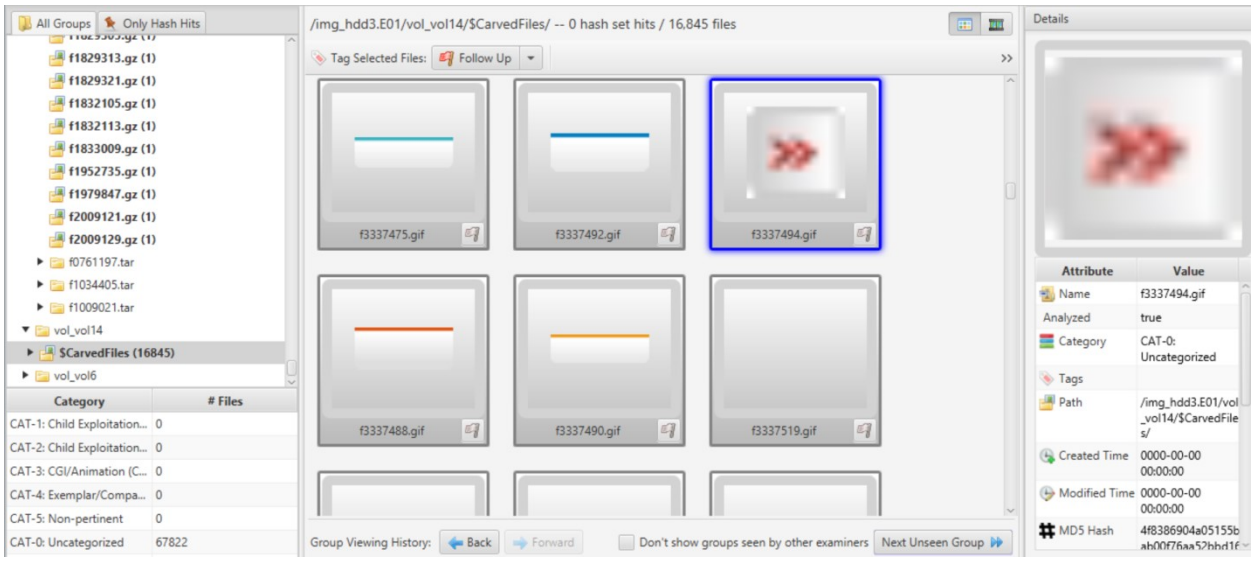


Fig. 48 Galeria e imazheve dhe videove në hard-diskun 3

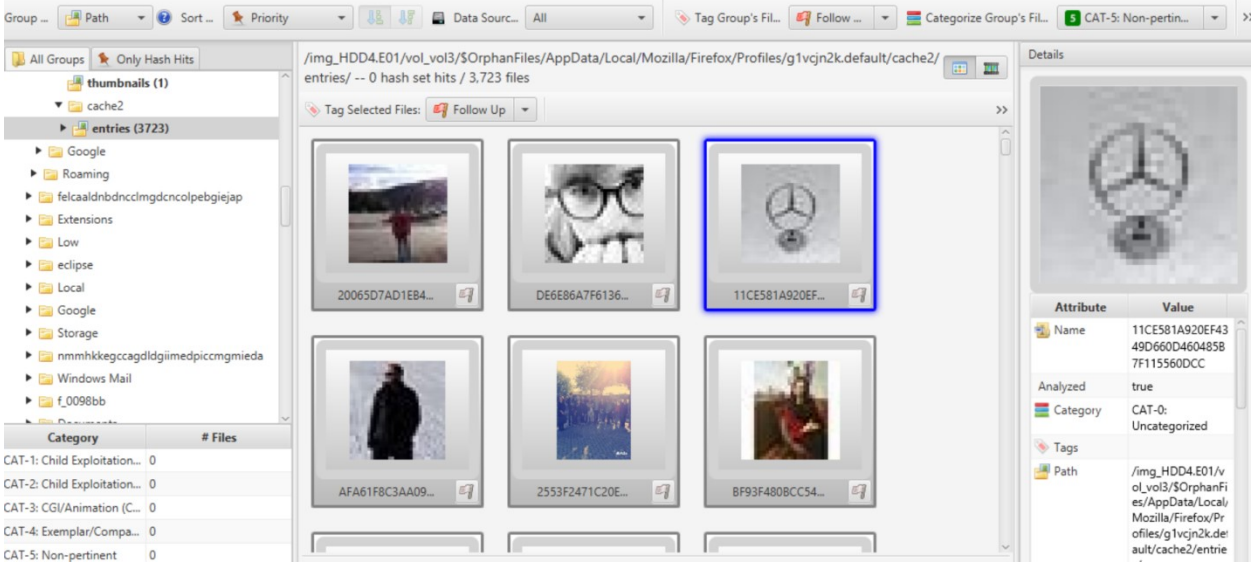


Fig. 49 Galeria e imazheve dhe videove në hard-diskun 4

3.14 Vizualizimi i komunikimit në *hard*-diskun 1

Pasi hapim dritaren komunikiuese të vizualizimit të komunikimit të *hard*-disukut nga kolona e majtë, mund të zgjedhim se cilat pajisje do të shfaqen, cilat lloje të të dhënave do të shfaqen dhe në mënyrë opcionale zgjedhim një interval kohor. Mund të kufizojmë ekranin vetëm në

komunikimet më të fundit. Pas çdo ndryshimi në filtra, përdoret butoni *Apply* për të azhuruar tabelat. Gjithashtu mund ta fshijmë këtë kolonë duke klikuar në shigjetën e majtë në krye të kolonës.

Kolona e mesit tregon llogaritë e kyçura, secilën llogari, pajisjen dhe llojin e saj, si dhe numrin e mesazheve shoqëruese (postat elektronike, regjistrat e thirrjeve, etj.). Si parazgjedhje, ai do të renditet sipas rendit zbritës të frekuencës. Shtylla e mesme dhe kolona e djathtë - të dyja kanë një tipar UI të kërkimit të shpejtë, i cili mund të përdoret për të gjetur shpejt një artikull të dukshëm në tabelën e seksionit në fjalë.

Përzgjedhja e një llogarie në kolonën e mesit do të sjellë të dhënat për atë llogari në kolonën e djathtë. Ka katër skeda që tregojnë informacion në lidhje me llogarinë e përzgjedhur.

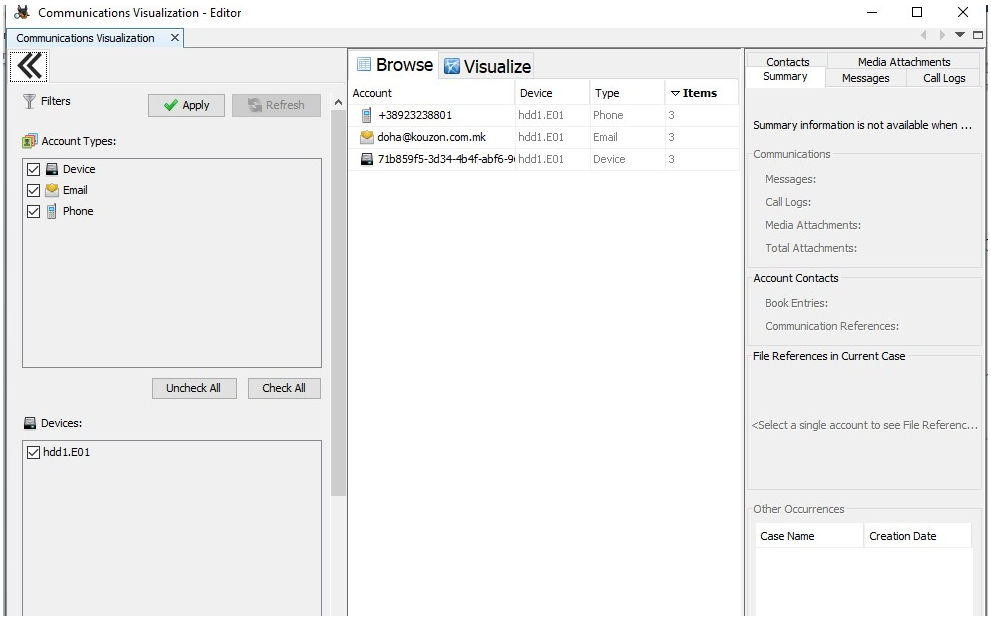


Fig. 50 Vizualizim i komunikimit në *hard*-diskun 1

Gjatë vizualizimit të komunikimit të hard-diskut ekzistojnë dy mundësi, të cilat janë ekuivalente nëse nuk është përzgjedhur asnjë llogari më parë:

- Shton llogarinë e zgjedhur dhe lidhjet e saj me grafin *(ang. Add Selected Account to Visualization);*
- Pastron grafin dhe shfaq vetëm lidhjet për këtë llogari *(ang.Visualize Only Selected Account)* (Anon., 2012).

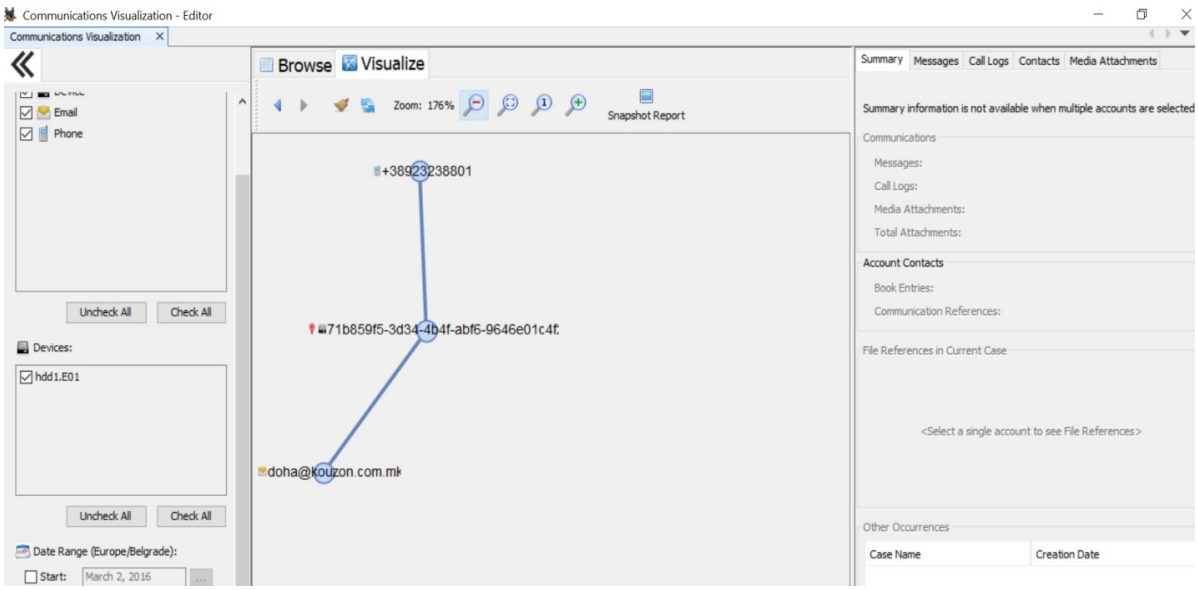


Fig. 51 Vizualizim i llogaris së përzgjedhur në *hard*-diskun 1

Opsionet e lartëpërmendura mundësojnë pastrimin e grafeve dhe gjithashtu mund të ndryshohet madhësia e grafit. Nyjet në graf mund të zvarriten përreth dhe nyjet dhe skajet mund të zgjidhen për të shfaqur mesazhet ose marrëdhëniet e tyre në skedën e anës së djathtë. Për shembull, në imazhin më poshtë është zgjedhur vetëm një nyje, kështu që shikuesi mesazheve po shfaq vetëm mesazhe që përfshijnë atë adresë emaili. (Anon., 2012)

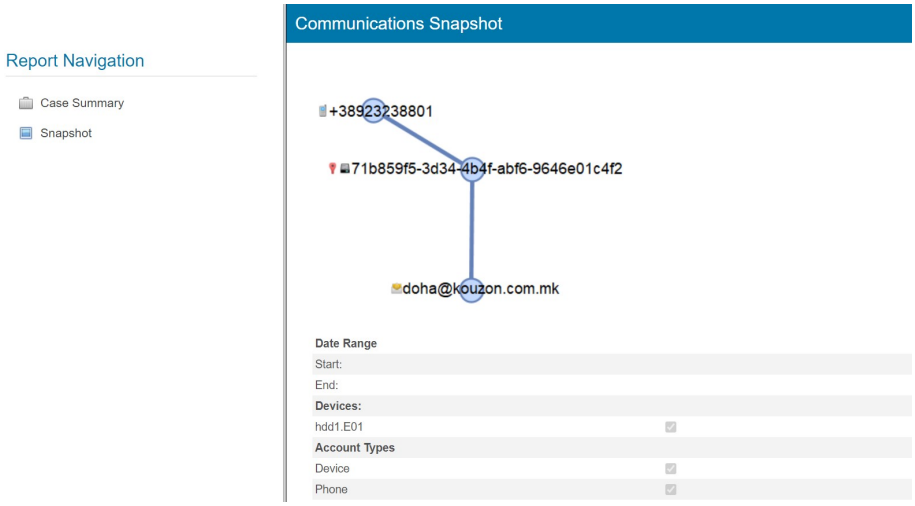


Fig. 52 *Snapshot raport* për nyje të caktuar në *hard*-diskun 1

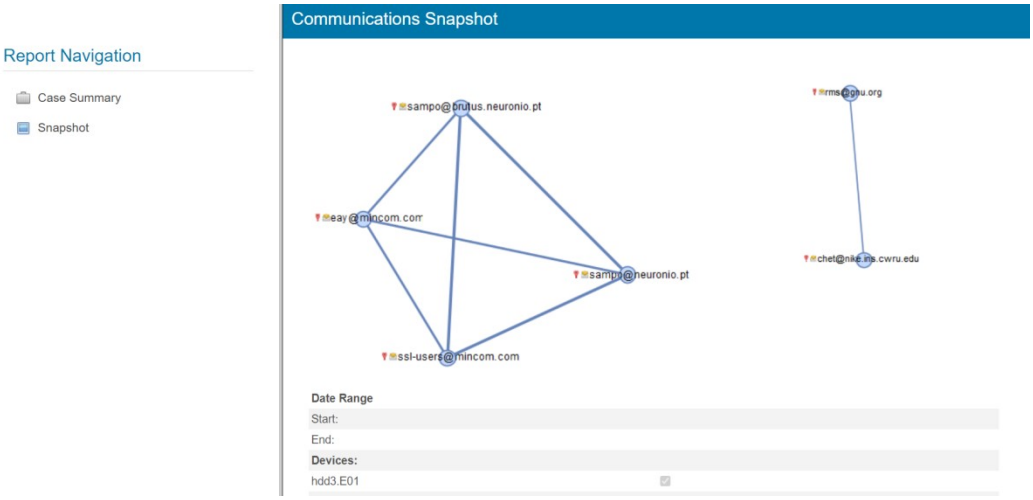


Fig. 53 *Snapshot raport* për nyje të caktuar në *hard*-diskun 3

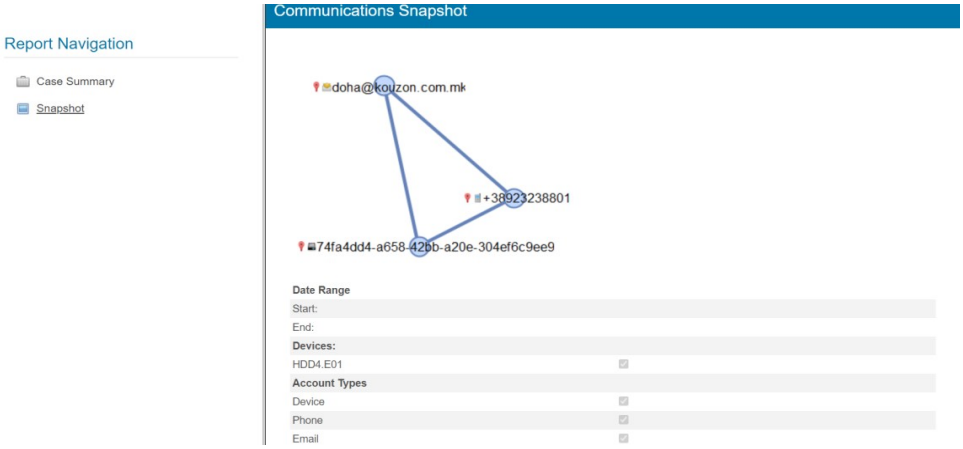


***Fig. 54 Snapshot raport* për nyje të caktuar në hard-diskun 4**

Hard*-disku 2 nuk posedon *snapshot raport për shkak se nuk ka pasur komunikime të kycura në PC.

Nëse klikoni në butonin "*Snapshot Report*", mund të krijoni një raport të ngjashëm me raportin e modul-it në HTML (ang. *report module*). Raporti i *Snapshot*-it përmbanë dy faqe. E para posedon një përmbledhje të rastit dhe e dyta përmbanë grafikun aktual së bashku me cilësimet e filtrit. (Anon., 2012)

3.15 Vendndodhja (ang. Geolocation) e fotografive në *hard*-diskun 1, 2, 3 dhe 4

Dritarja komunikuese e vendndodhjes (ang. *geolocation*) tregon objektet që kanë atributet e gjatësisë dhe gjerësisë si pika kalimi në hartë. Në këtë fushë, kur qasja në serverat e pllakave të hartave në internet mund të mos jetë e disponueshme, dritarja e vendndodhjes (geolocation) ofron mbështetje për burimet e të dhënave të pllakave (tile) të hartave *offline* (Anon., 2012).

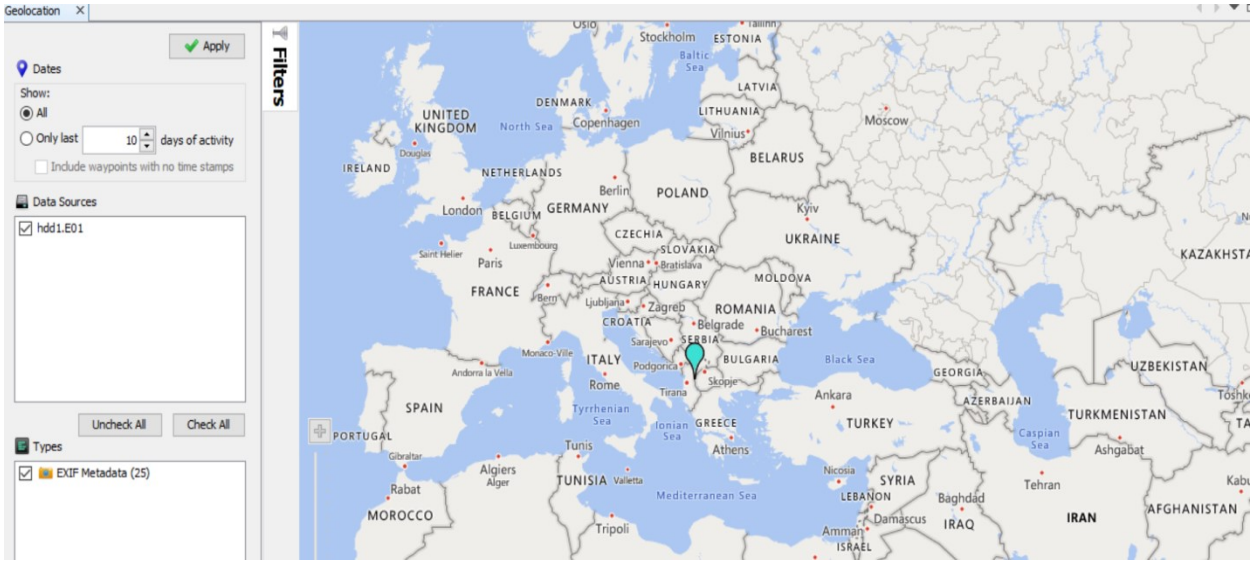


Fig. 55 Pamje nga vendndodhja (ang. geolocation) e fotografisë në hard-diskun 1

Më poshtë mund të shihni një fotografi, GPS koordinatat e saj, informata rreth kohës kur është bërë fotografia si dhe modeli i paisjes me të cilën është realizuar fotografia. Fotografia është gjetur përmes modulit *Picture Analyzer Module*.

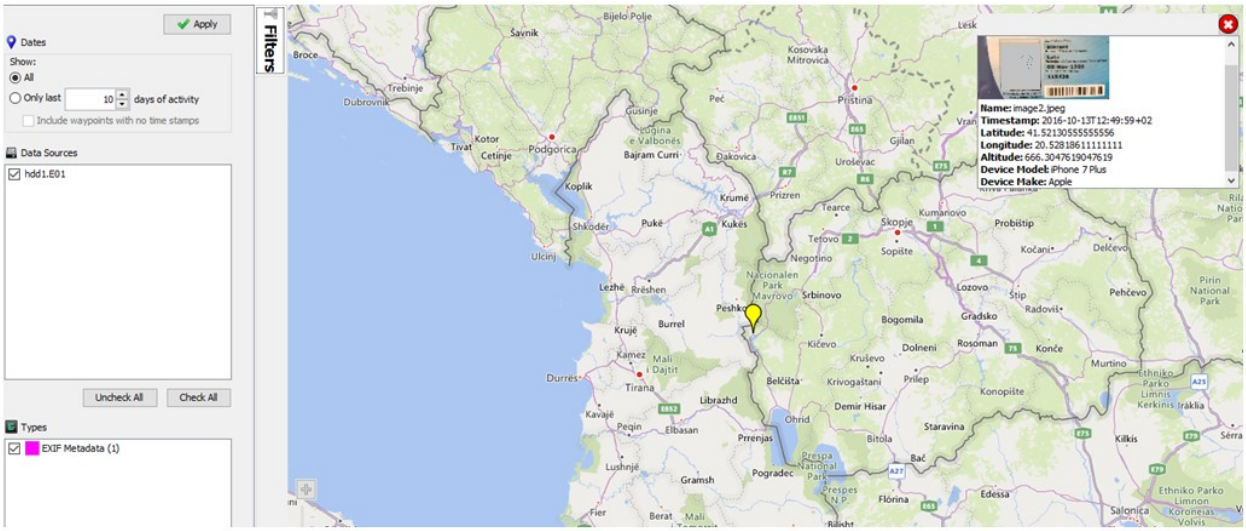


Fig. 56 Specifikacion i fotografijës nga *hard*-disku 1 përmes modulit *Picture Analyzer Module* nga vendndodhja (ang. *geolocation*)

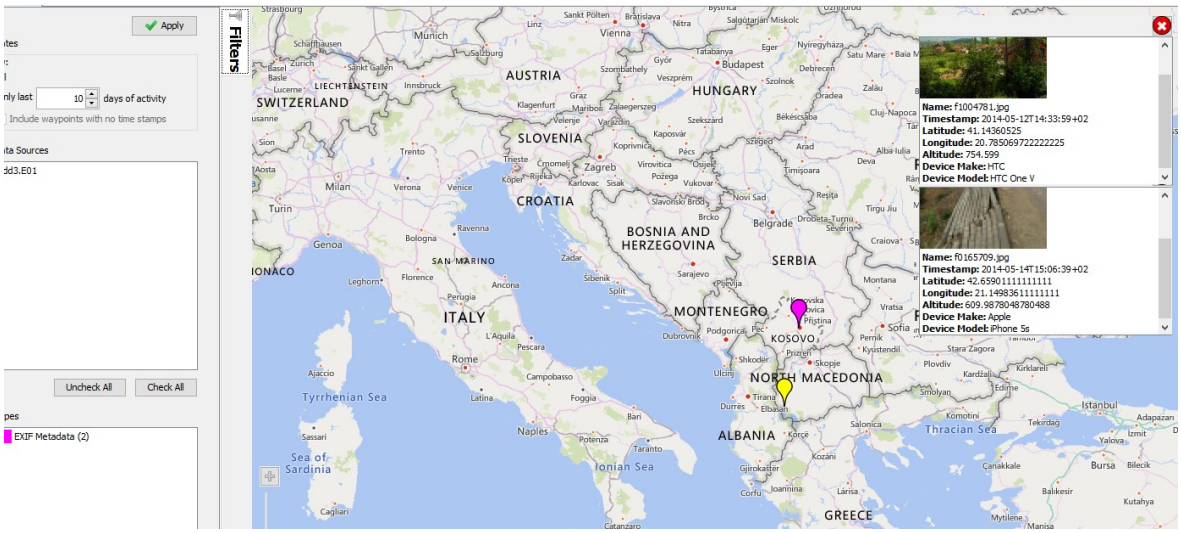


Fig. 57 Specifikacion i fotografive nga *hard*-disku 3 permes modulit Picture Analyzer Module nga vendndodhja (ang. *geolocation*)

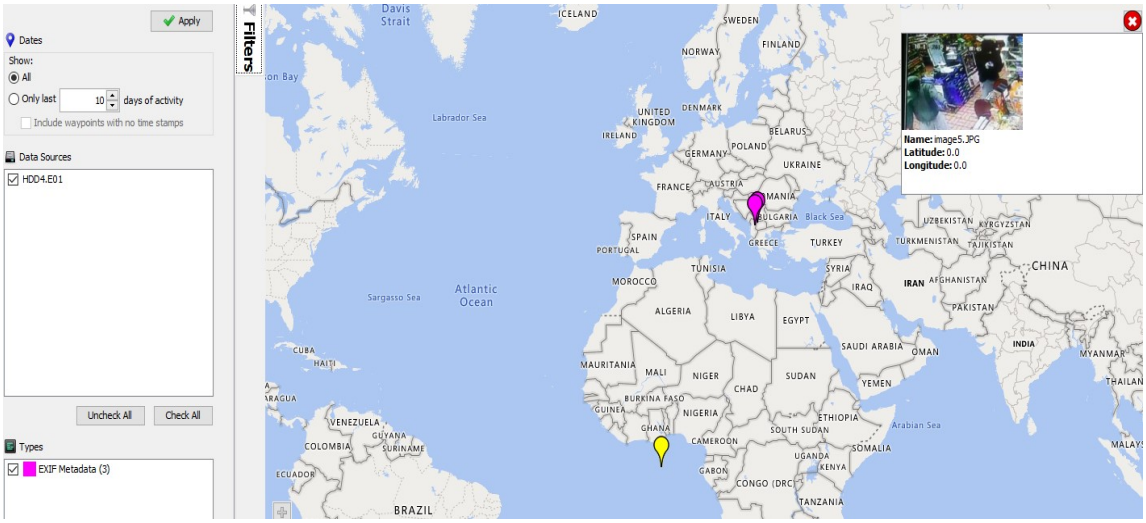


Fig. 58 Specifikacion i fotografijës nga *hard*-disku 4 permes modulit Picture Analyzer Module nga vendndodhja (ang. geolocation)

Në *hard*-disku 2 nuk u gjetën gjurmë të fotografive përmes modulit *Picture Analyzer Module* nga vendndodhja.

3.16 Vija kohore *(ang.Timeline)* e *hard*-diskut 1

Vija kohore *(ang.Timeline)* është proces i grumbullimit dhe analizimit të të dhënave të eventeve për të përcaktuar se kur dhe çfarë ka ndodhur në një sistem *file*-esh për qëllime gjurmuese. Rezultatet janë të organizuara në mënyrë kronologjike për të ilustruar një zinxhir të ngjarjeve në mënyrë koncize. (Anon., 2012)

Ekzistojnë tre lloje të ndryshme te paraqitjes grafike në vijë kohore të eventeve të ndodhura në një paisje të caktuar (hard-disk, usb, DVD etj) që ofron aplikacioni *Autopsy*, siç janë: pamja e numrit te *okurencave* (ang. counts view), pamja e detajeve (ang. *details view*) dhe pamja e listës (ang. *list view*). Në bazë të kërkesës së hetuesit, e cila paraqitje është më e përshtatshme për gjurmimin e tij për at lloj, edhe përcaktohet hetuesi.

Pamja e numrit te *okurencave* (ang. *counts view*) tregon të gjitha aktivitetet e ndodhura të grumbulluara në paraqitje grafike. Përdorim i këtij lloj grafiku tregon se sa aktivitete kanë

ndodhur në një kornizë kohore të caktuar. Mund të jetë shumë e dobishme nëse është e nevojshme të përcaktohet se kur është përdorur kompjuteri për herë të fundit, ose sa shpesh është përdorur. Kur hapim kronologjinë e kërkuar, ajo duket si në figuren 59.

Vija kohore fillon nga pamja e numrit të okurencave (ang. ***counts view***) përmes paraqitjes grafike ku tregohet numri i ngjarjeve në çdo periudhë kohore.

Vija kohore mund të ndihmojë në përgjigjen e pyetjeve të tilla si:

- Kur ka ndodhur një ndër ueb aktivitetet më kryesore në sistem?

- Kur janë kyçur paisje të jashtme në sistem?

- Kur janë shtuar fotografitë me EXIF informacion?

- Cilat uebfaqe u qasën që më pastaj rezultuan modifikimet e sistemit të *file*-eve?

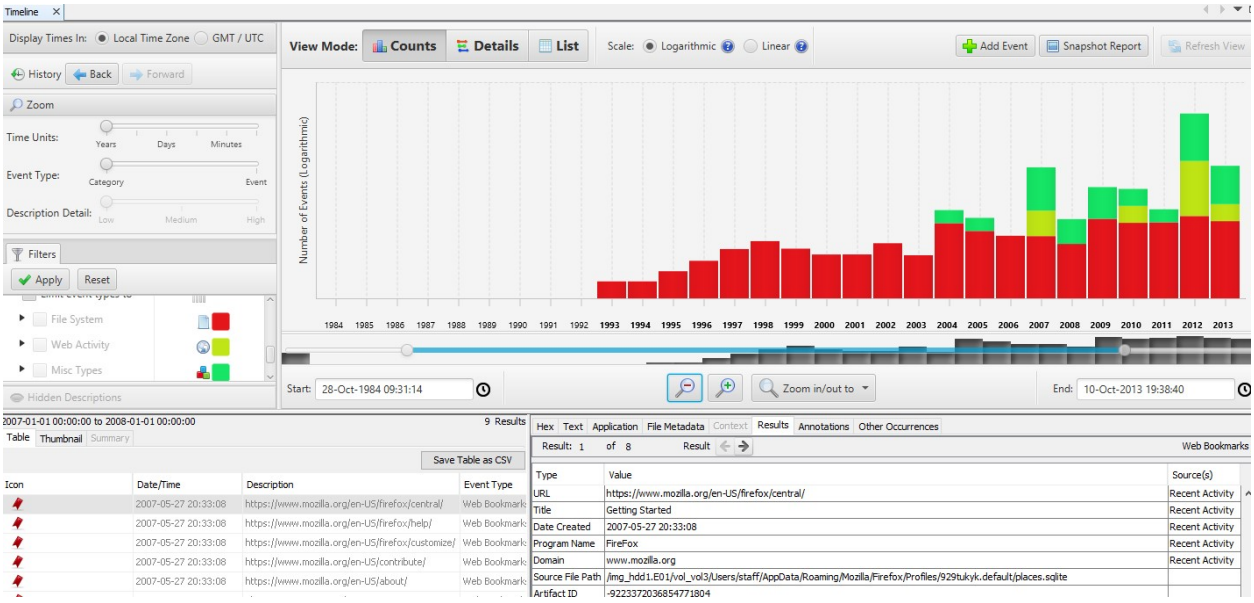


Fig. 59 Vija kohore (ang.Timeline) e hard-diskun 1 përmes pamjes *Counts View*

Në figurën 59 mund të shihet pamja e numrit të *okurencave* për hard-diskun 1. Me ngjyrë të kuqe janë paraqitur ngjarjet nga *file* sistem-i, me ngjyrë te verdhë janë paraqitur ngjarjet nga ueb aktivitetet (ang. *Web Activites*) dhe me ngjyrë të gjelbert janë paraqitur eventet e ndryshme (ang. *Misc Types*).

Nëse klikojmë në njërin nga segmentet e grafeve, do të na shfaqet lista e ngjarjeve në të majtë poshtë, ndërsa detajet e eventit shihen në dritaren në të djathtë poshtë.

Në pjesën e poshtme të dritares mund të përzgjedhim një periudhë kohore të caktuar për të cilën dëshirojmë të na shfaqet pamja e *okurencave*. Në figurën 60 mund të vërrejmë të njejtën.

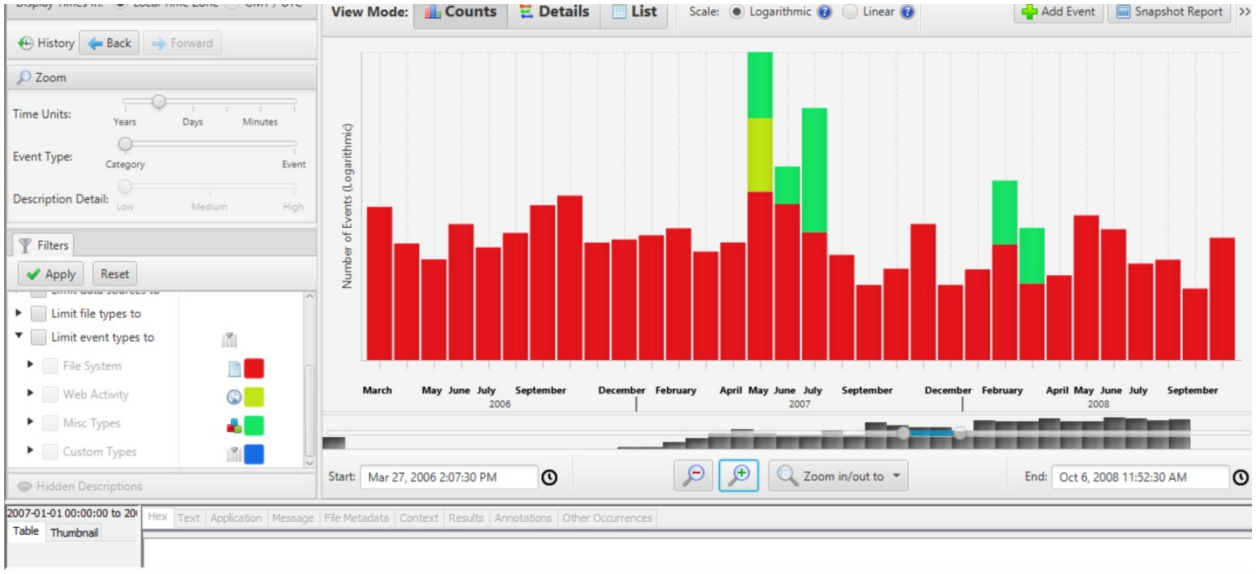


Fig. 60 Pamje e vijës kohore të hard-diskut 1 duke përzgjedhur një periudhë kohore të caktuar.

Mund të ndryshohet pamja e vijës kohore duke përdorur butonat në zonën e mesme të sipërme të dritares. Modaliteti i dytë i pamjes - pamja e detajeve (ang. *Details view)*, tregon informacion mbi ngjarjet që kanë ndodhur në një periudhë specifike kohore. Paraqitjen e pjesërishme mund ta shihni përmes figurës në vijim:

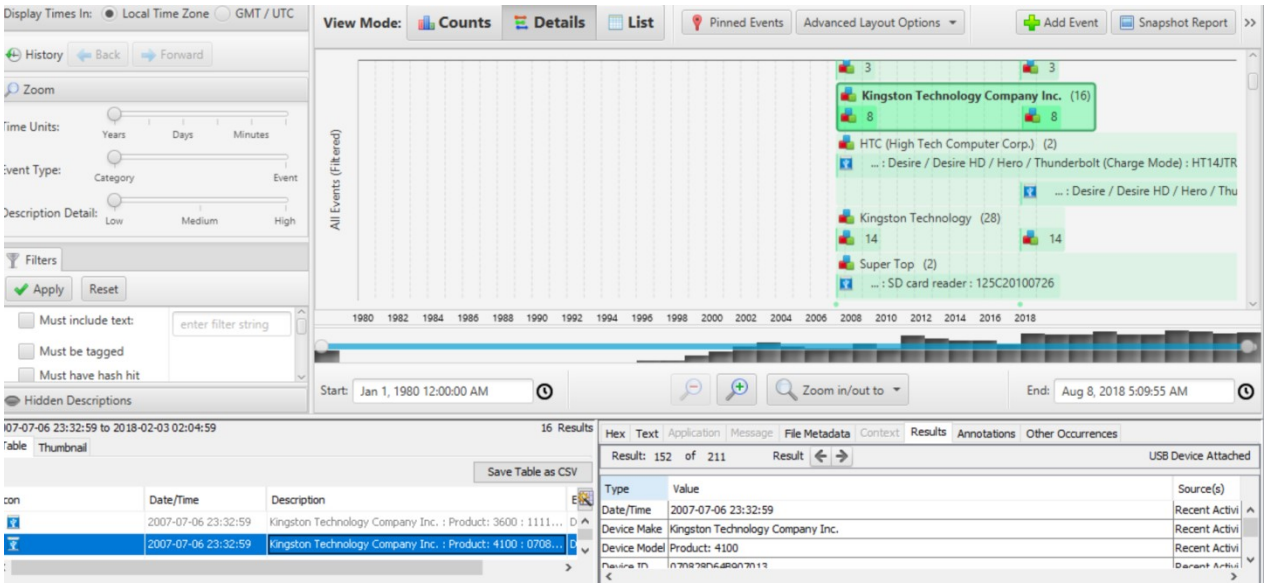


Fig. 61 Modaliteti i dytë i pamjes të vijës kohore të hard- diskut 1 përmes pamjes së detajeve (ang. Details view)

Modalitet i pamjes përfundimtare të vijës kohore të hard-diskut 1 është pamja e listës (ang. *List view)*. Kjo pamje tregon çdo ngjarje në bazë kronologjike. Kjo pamje mund të jetë e dobishme për të parë se cilat ngjarje të tjera kanë ndodhur në të njëjtën kornizë kohore si ngjarje me interes. Sikurse me pamjen e detajeve (details view), edhe pamja e listës (list view) përdoret më së miri duke shfrytëzuar filtrat për të zvogëluar numrin e ngjarjeve të treguara. Të njëjtën mund ta vëreni ne figurën 62.

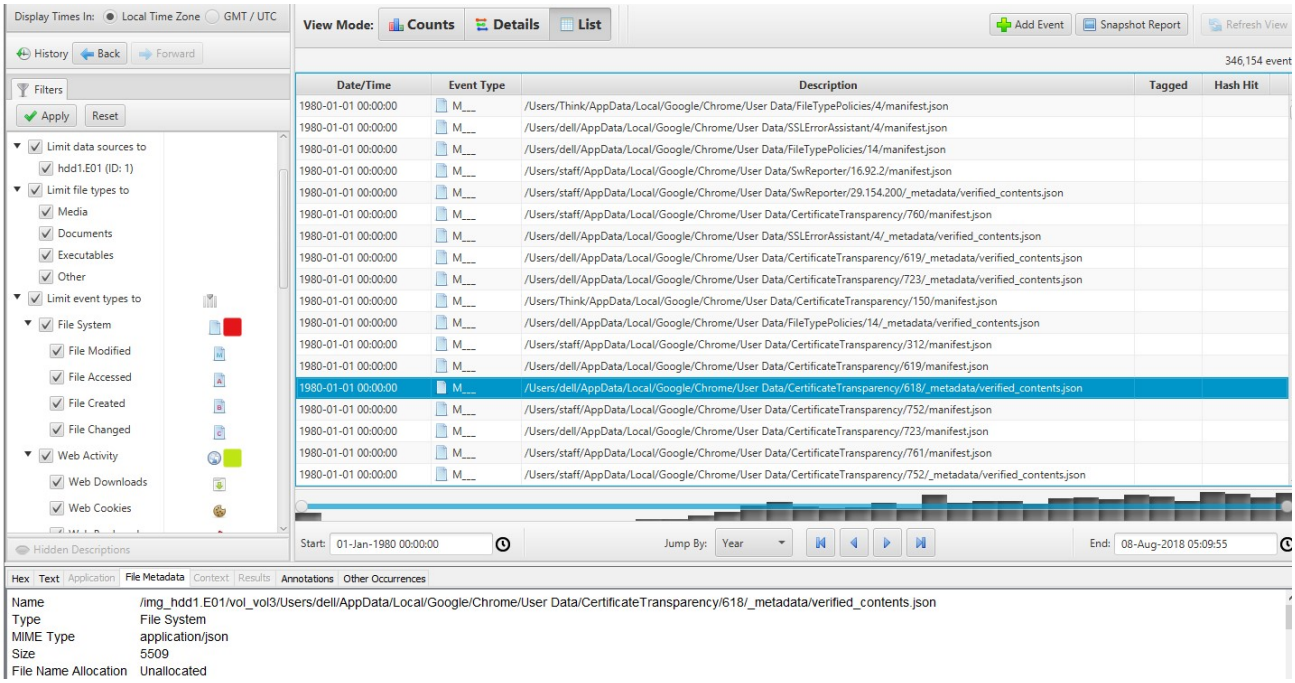
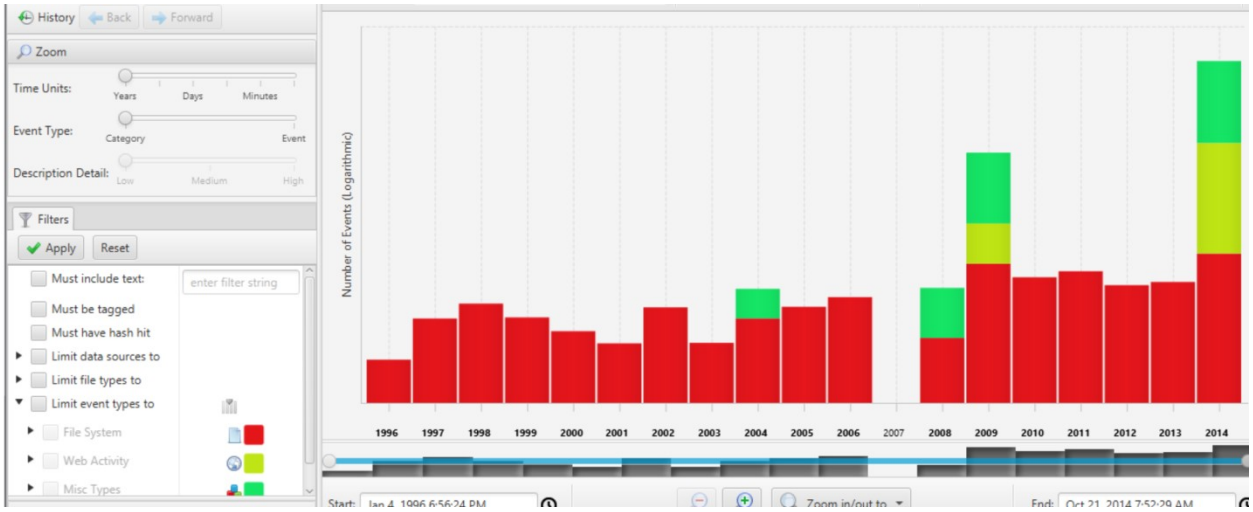
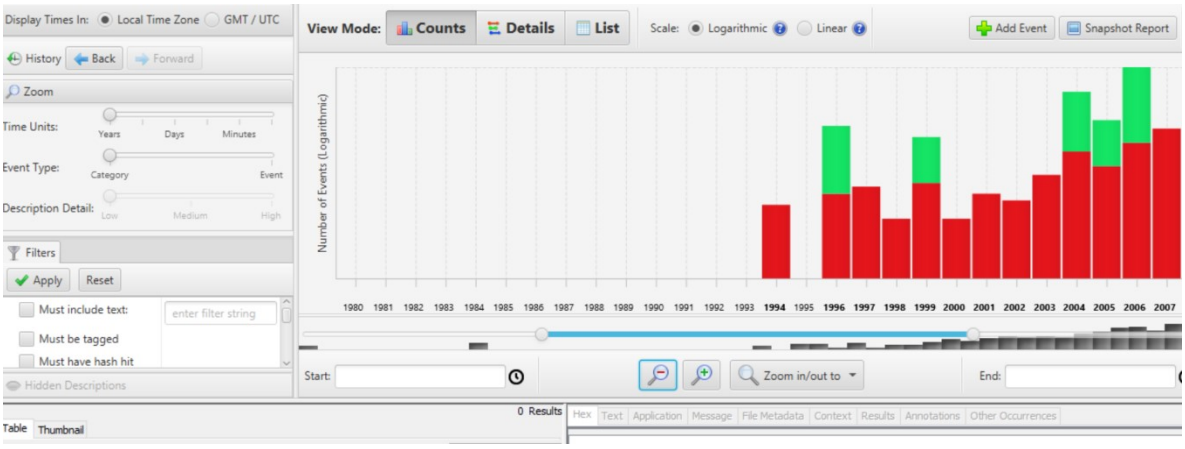


Fig. 62 Modaliteti i tretë i pamjes të vijës kohore të hard- diskut 1 përmes pamjes së listës (ang. List view)

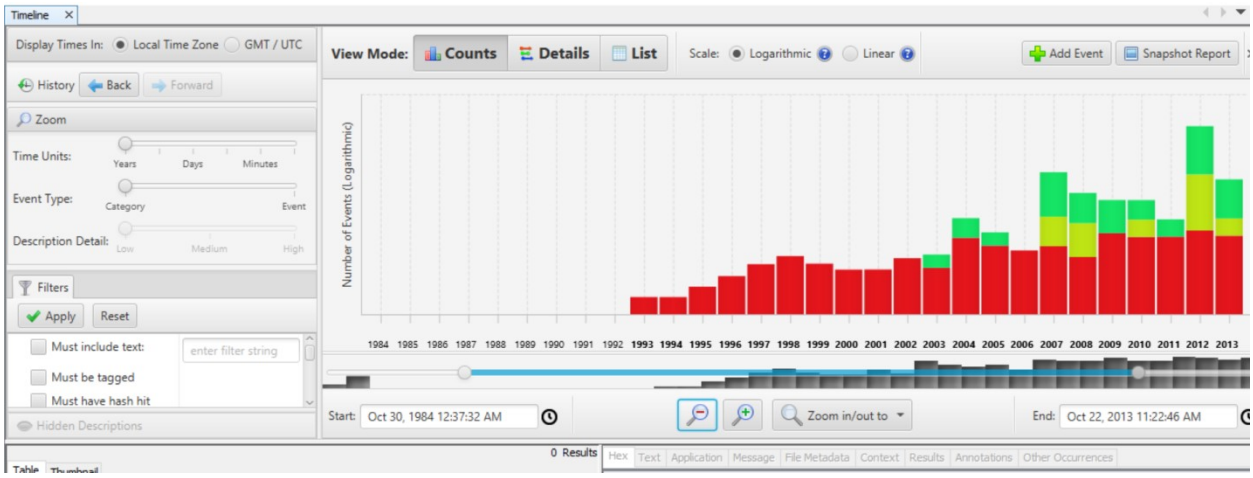
Gjatë analizës së vijës kohore të *hard*-disqeve 2, 3 dhe 4 u përsëritën etapat e lartëpërmendura sikurse gjatë gjenerimit të vijës kohore për hard-diskun 1. Në vijim shihet qartë pamja e vijës kohore të hard-disqeve 2,3 dhe 4 duke përzgjedhur pamjen *Count*.



***Hard*-disku 2**



***Hard*- disku 3**



***Hard*- disku 4**

Fig. 63 Pamje e vijës kohore të *hard*-disqeve 2, 3 dhe 4 duke përzgjedhur pamjen *Count*

3.17 Zbulim i *file*-eve (ang. *File Discovery*)

Vegla e zbulimit të *file*-eve tregon imazhe, video, dokumente ose domene që përputhen me një grup filtrash të konfiguruar nga përdoruesi. Ne mund të zgjedhim se si ti grupojmë dhe rradhisim rezultatet e shfaqura në mënyrë që të shohim më parë të dhënat më të rëndësishme.

Kur klikohet në opsionin zbulim i *file*-eve (ang. File Discovery), na shfaqen këta tre hapa:

1. Zgjedhja e llojit të rezultatit (ang. Choose the result type);

2. Vendosja e filtrave (ang. Set up filters);
3. Zgjedhja e mënyrës së grupimit dhe renditjes së rezultateve (ang. *Choose how to group and sort the results).*

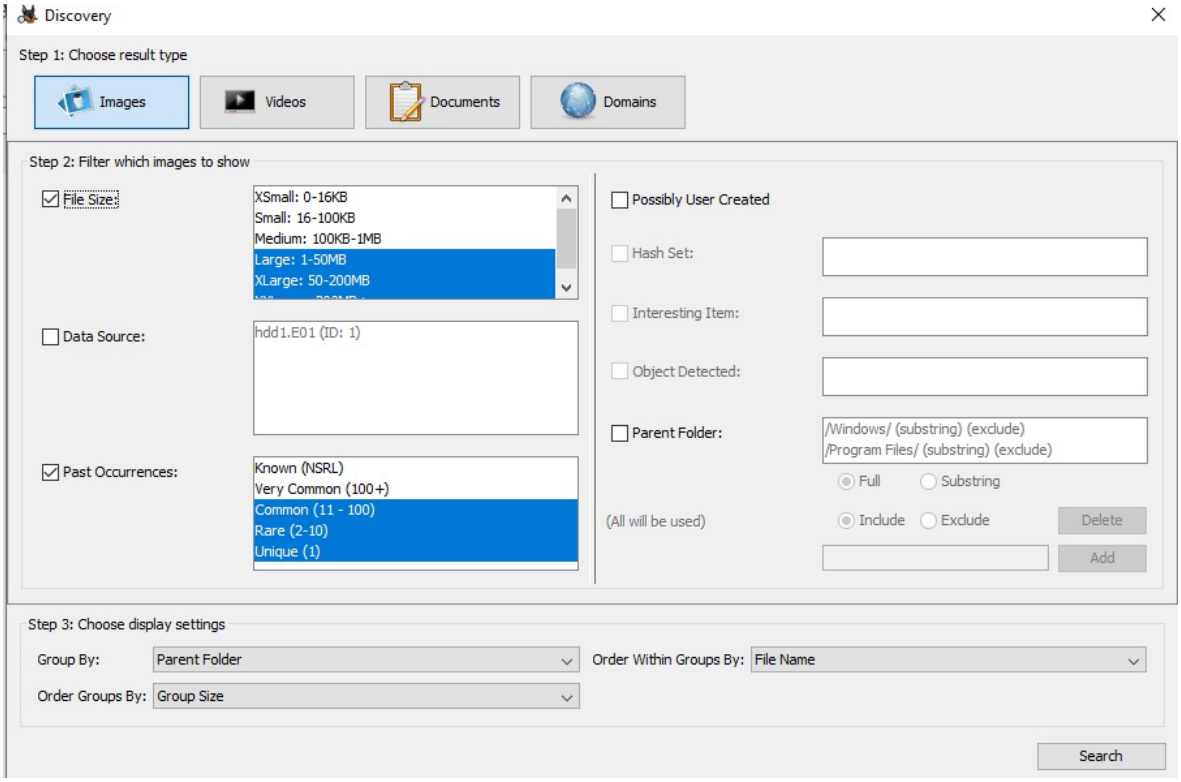


Fig. 63 Dritarja komunikuese pas përzgjedhjes së opsionit zbulim i file-eve (ang.File Discovery)

Së pari përzgjedhim llojin e analizimit të *file*-ve që dëshirojmë të zbulojmë, në rastin konkret na shfaqen mundësitë për kategoritë: imazhe (ang. *Images*), video (ang. *Video*), dokumente (ang. *Documents*) dhe domene (ang. *Domains*). Në fillim përzgjedhim kategorinë Imazhe (ang.*Images*). Me pastaj si hap të dytë bëjmë përzgjedhjen dhe konfigurimin e filtrave. Shumicën e filtrave i aktivizojmë duke përdorur kutinë e zgjedhjes në të majtë dhe më pas zgjedhim opsionet që dëshirojmë.

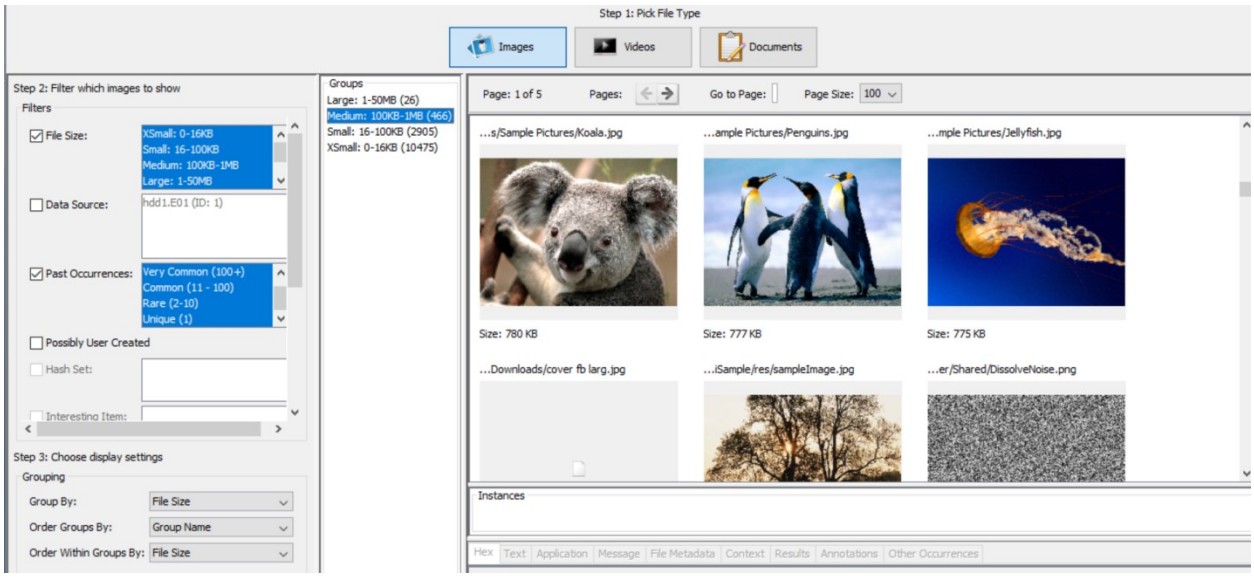


Figure 64 Zbulim i file-eve (ang.file discovery) - kategorija imazhe të hard diskut 1

Hapi i dytë është zgjedhja dhe konfigurimi i filtrave. Në rastin konkret pas percaktimit të filtrave na shfaqet dritarja si në figurën 66 me imazhet e kërkuara të kategorizuara në grupe në bazë të madhësisë: për 1-50 MB janë detektuar 26 imazhe; për 100 KB-1 MB janë detektuar 466 imazhe; për 16-100 KB janë detektuar 2905 imazhe dhe nga 0-16 KB janë detektuar 10475 imazhe.

Hapi i tretë është përzgjedhja e cilësimeve të ekranit (ang. *Choose display settings*). E njejta procedure përsëritet edhe për kategorinë video, dokumente dhe domene.

Përmes shfrytëzimit të veglës zbulim i *file*-ve në bazë të kërkesës, investiguesit mund të arrijnë shumë më shpejtë deri në file-in e kërkuar duke shfrytëzuar kategoritë që janë në dispozicion në dritaren komunikuese të veglës zbulim i *file*-eve.

3.18 Gjenerim i raportit

Moduli i gjenerimit të raportit i mundëson përdoruesit të nxjerrë informacionet kryesore të një rasti (ang.*case*) në një larmi formatesh. Kjo përfshin gjenerimin e një raporti në formatin HTML

ose *Excel* që përmban të gjithë përmbajtjen e nxjerrë, etj. nga një rast, ose krijimin e një *file*-i KML nga çdo koordinatë e gjetur, të ngarkohet në softuer si Google Earth.

Raportet e gjeneruara mund ti gjejmë në nyjen *Reports*, të paraqitur në figurën 67.

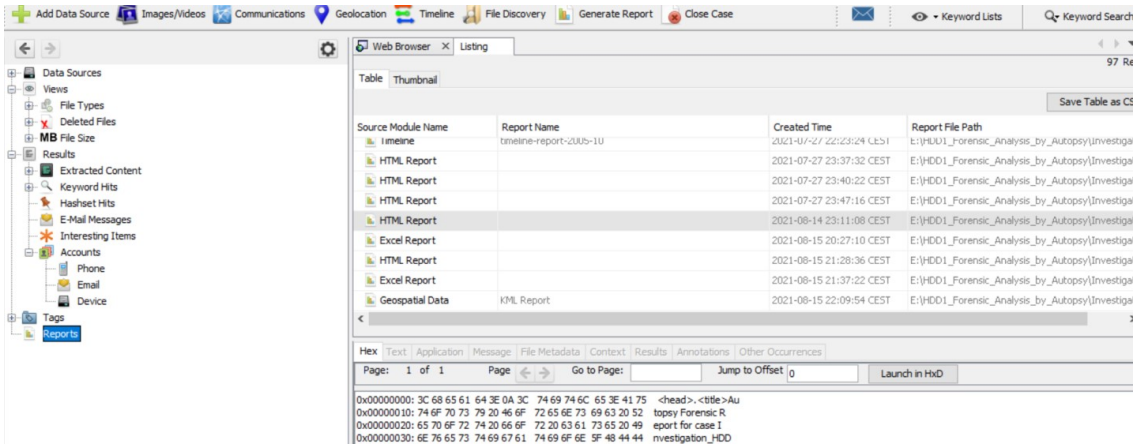


Fig. 65 Raportet e gjeneruara të vendosura në nyjen *Reports*

Egzistojnë disa lloje të raporteve që mund të gjenerohen përmes modulit për gjenerimin e raportit, siç janë: *HTML* raport, *Excel* raport, *Files- text* raport, *Save Tagged Hashes* raport, *TSK Body File* raport, *Google Earth KML* raport, *STIX* raport, *Case-Uco* raport dhe *Portable Case* raport. Llojet e raporteve gjatë gjenerimit të raportit mund ti shihni edhe nga dritarja në figurën 68:

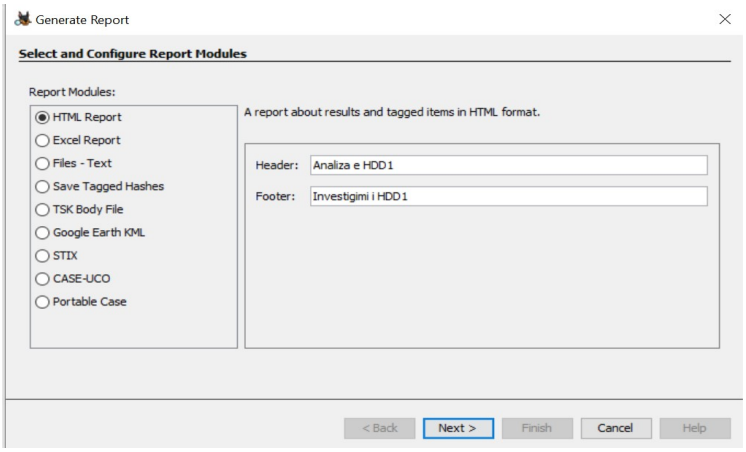


Fig. 66 Llojet e raporteve që mund të gjenerohen përmes modulit për gjenerimin e raportit (ang. *Generation report*)

Gjatë gjenerimit të raportit mund të bëjmë përzgjedhjen e llojit të raportit si dhe të kategorive: të gjitha rezultatet (ang.All results), ose rezultatet e *tag*-uara (ang.Tagged results).

Gjatë gjenerimit të *HTML* raportit, përzgjedhëm kategorinë - të gjithë rezultatet. Më poshtë në figurën 69 mund të gjeni *HTML* raportin e gjeneruar për *hard*-diskun 1 duke përzgjedhur të gjitha rezultatet.

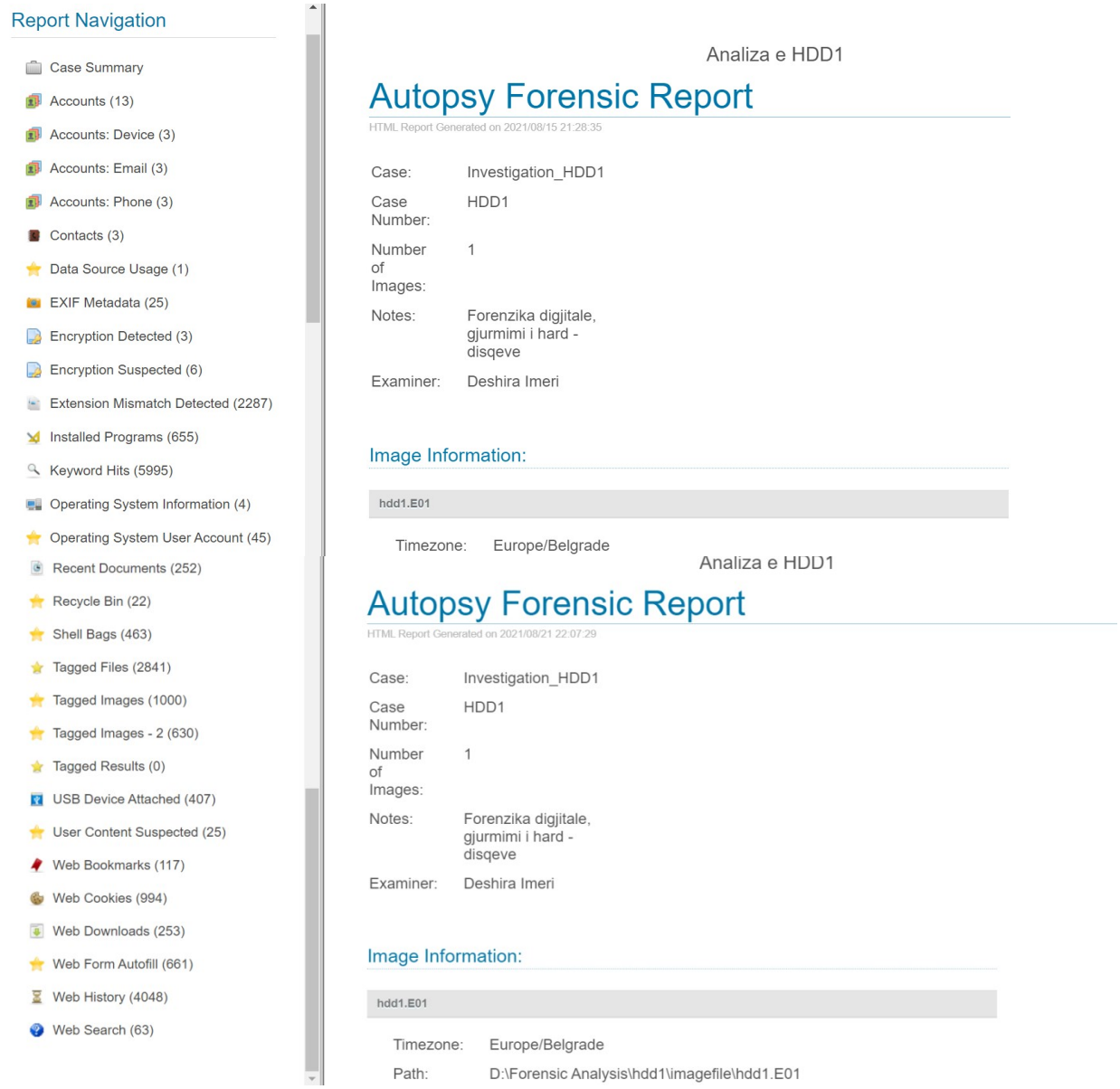


Fig. 67 *HTML* raport i gjeneruar për hard-diskun 1

Në anën e majtë të dritares në figurën 69 shihen të gjitha linqet të cilat mund ti shfrytëzojmë për të parë rezultatet e të dhënave të kategorizuara.

Gjenerim i raporteve të llojit HTML u gjeneruan edhe për *hard*-disqet 2, 3 dhe 4.

3.19 Krijimi i imazhit forenzik tek *hard*-disku fizikisht i dëmtuar

Deri më tani, ka pasur vetëm një numër të kufizuar të studimeve në lidhje me problemin e rikuperimit të të dhënave të *Drive*-ve të *Hard* Disqeve (HDD) dhe *Solid-State Drive*-ve (SSD), ku dizajni i brendshëm i *hard* disqeve moderne mund të parandalojë ose zvogëlojë rrezikun e humbjeve të të dhënave edhe në rrethana ekstreme. Gjithashtu, janë krijuar edhe HDD dhe SSD moderne për të siguruar të dhënat në kushte të ndryshme, edhe nëse kryerësi është duke përdorur një forcë të madhe dhe ku pjatat magnetike brenda kompjutorëve mund të mbeten të paprekura (Solodov & Solodov, 2021).

Sipas analizës së Solodov et.al., (2021) të cilët kanë marrë në hulumtimin e tyre 14 disqe për analizë dhe të njëjtat iu nënshtruan dëmtimeve nga zjarri, dëmtimeve nga uji, por edhe goditjeve dhe dridhjeve të ndryshme, pas rezultateve të fituara kanë arritur në disa konkluzione.

Solodov et. al., (2021) përkufizuan se mundësia e rikuperimit të suksesshëm të të dhënave në rastin e HDD-ve dhe SSD-ve me shenja të dëmtimit nuk duhet të përjashtohen bazuar në pamjen vizuale të pajisjes. Është e rëndësishme të përfundoni rikuperimin e të dhënave brenda një kohe të shkurtër. Rikuperimi selektiv i të dhënave është një metodë e preferuar.

Në këtë studim, pas krijimit të katër imazheve forenzike për *hard*-disqet 1, 2, 3 dhe 4, u testua gjithashtu krijimi i imazhit forenzik tek *hard*-disku fizikisht i dëmtuar, me ç'rast u konkludua se përmes veglës për krijim të imazheve forenzike digjitale FTK *Imager* nuk mund të gjenerohet imazh forenzik kur hard-disku është fizikisht i dëmtuar.

4. PËRFUNDIME DHE REKOMANDIME

Në kuadër të këtij punimi është hulumtuar aspekti forenzik digjital, si njëra nga arsyet e evoluimit të krimit në përgjithësi, është kryer gjurmimi i *hard*-disqeve si dhe është bërë mbledhja dhe analiza e të dhënave nga Ministria e Punëve të Brendshme në Republikën e Maqedonisë së Veriut (RMV) sa i takon krimit kompjuterik, për ti krahasuar me praktikat më të mira bazuar në teori dhe sistemet më të reja, për të nxjerrur rekomandimet për përmirësim eventual.

Në bazë të hulumtimeve dhe analizave të bëra mund të konkludohet se si shkaktarë të rritjes se veprave penale dhe kryerësve të krimeve kompjuterike në vend janë faktor të ndryshëm, e si më kryesori është zhvillimi teknologjik, ndërsa determinantë tjetër është edhe rritja e përdoruesve të internetit në RMV gjatë kësaj peiudhe kohore.

- Numri më i lartë i veprave penale (174) është regjistruar në vitin 2019. Karakteristikë e veçantë është se vërehet një trend pozitiv linear gjatë dekadës së fundit.
- Numër më të madh të krimeve kompjuterike sipas Ligjit për Procedurë Penale janë: "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik", me 267 vepra penale, si dhe "ngacmim seksual ndaj një fëmije nën 14 vjeç", me 230 vepra penale.
- Llojet e krimeve kompjuterike më të shprehura në RMV gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 janë: rrezikimi i sigurisë; abuzimi i të dhënave personale; dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik, i cili gjatë periudhës kohore prej vitit 2016 deri në vitin 2019 ndjek një mesatare rreth 46 shkelje të paautorizuara për një vit; si dhe mashtrimet kompjuterike që janë regjistruar, janë me një mesatare rreth 11 vepra penale gjatë një viti.
- Gjatë periudhës 2010-2014 janë regjistruar 211 krime kompjuterike në qytetin e Shkupit. Krimi më i shprehur është "dëmtimi dhe hyrja e paautorizuar në një sistem kompjuterik" te të gjitha SPB-të në RMV. Ndërsa, sa i përket raporteve të krimeve kompjuterike, meshkujt prijnë trefish më shumë se sa gjinia femërore në RMV - gjatë periudhës së hulumtimit. Sipas moshës, shumica e personave të regjistruar në periudhën e përmendur

janë midis 25 dhe 29 vjeç, të ndjekur nga personat e moshës 18-24 vjeçare. Sipas përqindjeve kumulative, pak më shumë se 58% e personave të raportuar në periudhën e vëzhgimit janë nën 30 vjeç.

Sipas Indeksit Global të Sigurisë Kibernetike në Evropë (itu.int, 2017), i cili paraqet një analizë të Sigurisë Kibernetike për rajonin e Evropës, RMV rrezullton në nivelin mesatar sipas Indeksit Global të Sigurisë Kibernetike.

Në bazë të parametrave matës sipas Indeksit Global të Sigurisë Kibernetike në Evropë rezulton që në RMV duhet përmirësuar disa nga shtyllat e sigurisë edhe atë: masta ligjore, teknike dhe organizative me qëllim që krimi kompjuterik të ketë ulje në vendin tone.

Në lidhje me forenzikën digjitale, gjurmimin e *hard*-disqeve, krijimin dhe analizimin e imazheve forenzike janë përdorur veglat FTK Imager dhe Autopsy 4.15.0

Rëndësi të madhe ka edhe kyçja e paisjes *Tableau eSata Forensic Brige* i cili është një bllokues i lëvizshëm portativë (ang. *portable*) i të shkruarit që mundëson përvetësimin forenzik të *hard*-disqeve SATA.

Përmes veglës Autopsy, për analizë të imazheve forenzike, mund të kthehen të gjitha gjitha *file*-et e fshira, apo të *tag*-ohen vetëm disa nga file-et që janë në interes të palës. Cilësia e *file*-ve të fshira edhe pas kthimit mbetet e lartë.

Numri i *file*-ve të allokuar në një imazh forenzik nuk luan rol në kohëzgjatjen e gjenerimit të raporteve gjatë krijimit të imazheve forenzike përmas FTK *Imager*.

Për dallim të *file*-ve të allokuar, *file*-et e pa analizuara në një imazh forenzik janë në proporcion të drejtë me kohëzgjatjen e gjenerimit të raporteve për imazhet forenzike përmes FTK *Imager.*

Në këtë studim, pas krijimit të katër imazheve forenzike për *hard*-disqet 1, 2, 3 dhe 4, është testuar gjithashtu krijimi i imazhit forenzik tek hard-disku fizikisht i dëmtuar, me ç'rast është përfunduar se permes veglës për krijim të imazheve forenzike digjitale FTK *Imager* nuk mund të gjenerohet imazh forenzik kur hard-disku është fizikisht i dëmtuar.

Si përfundim dhe rekomandim mund të thuhet se veglat me burim të hapur (ang. *open source*) për krijim dhe analizim të imazheve forenzike FTK Imager dhe Autopsy 4.15.0 janë shumë efikase në gjurmimin e hard-disqeve, por nuk mund të krijojnë dhe analizojnë imazhe forenzike tek hard- disqet fizikishtë të dëmtuara, andaj edhe duhet shfrytëzuar vegla që mundësojnë leximin magnetik të *hard*- disqeve fizikisht të dëmtuara.

BIBLIOGRAFIA

(2021, 06 21). Retrieved from Live Stat: https://www.internetlivestats.com/internet-users/#trend

(2021, 06 22). Retrieved from United Nations: https://ccdcoe.org/organisations/un/

(2021, 06 30). Retrieved from sleuthkit.org: https://www.sleuthkit.org/

(2021, 06 30). Retrieved from The Sleuth Kit: The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools

(2021, 06 30). Retrieved from sleuthkit.org: https://sleuthkit.org/autopsy/docs/user-docs/3.1/workflow_page.html

(2021, 06 30). Retrieved from sleuthkit.org: https://sleuthkit.org/autopsy/docs/user-docs/3.1/index.html

(2021, 06 30). Retrieved from sleuthkit.org: https://sleuthkit.org/autopsy/docs/user-docs/3.1/ds_page.html

(2021, 06 30). Retrieved from sleuthkit.org: https://sleuthkit.org/autopsy/docs/user-docs/3.1/quick_start_guide.html

(2021, 06 30). Retrieved from digitalcorpora.org: https://digitalcorpora.org/corpora/disk-images/real-data-corpus

AccessData Group, Inc. (2017 , April 3). *Access Data.* Retrieved august 11, 2020, from https://ad-pdf.s3.amazonaws.com/ftk/7.x/FTK_UG.pdf

Anstee, D. (2012). *Worldwide Infrastructure Security Report.* Arbnor Networks.

Arnes, A. (2018). *Digital Forensics.* John Wiley & Sons Inc.

Ayers, R., Brothers, S., & Jansen., W. (2014). Guidelines on Mobile Device Forensics. *NIST Special Publication, 1(1):85*.

Balogun, A. M., & Zuva, T. (2017). OPEN ETHICAL ISSUES IN DIGITAL FORENSIC SYSTEMS. *INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES, Vol 9, No 1*.

Barnett, P. D. (2001). *Ethics in Forensic Science: Professional Standards for the Practice of Criminalistics.* Boca Raton, FL: CRC Press.

Boddington, R. (2016). *Practical Digital Forensics.* Packt Publishing Ltd.

Breitinger, C. G., & Baggili, I. (2017). Availability of Datasets for Digital Forensics–and What is Missing. *Cyber Forensics Research and Education Group (UNHcFREG), Tagliatela College of Engineering, ECECS, University of New Haven, 300 Boston Post Rd., WestHaven, CT 06516, USA*.

Casey, E. (2011). *Digital Evidence and Computer Crime.* Elsevier.

Castillo, A. C. (2019). Network Forensics: Concepts and Challenges. *Journal of Forensic Science & Criminal Investiagtion*.

ccdcoe.org. (2021, 06 22). *ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.* Retrieved from ict4peace.org: https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

Chopade, R., & Pachghare, V. (2019). Digital Investigation: Ten years of critical review on database forensics research. *Elsevier*, 180-197.

Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F., & Daryabar, F. (2013). Digital Forensic Trends & Future. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 2, no. 2*, 48–76.

Digital Corpora. (2019, 04 22). Retrieved from https://digitalcorpora.org/corpora/disk-images/real-data-corpus

Du, X. (2020). *Alleviating the Digital Forensic Backlog: A Methodology for Automated Digital Evidence Processing.* Dublin: UCD School of Computer Science, College of Science, University College Dublin.

Du, X., Ledwith, P., & Scanlon, M. (2018). Deduplicated Disk Image Evidence Acquisition and Forensically-Sound Reconstruction. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications* (pp. 1674-1679). 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *ArXiv, abs/1708.01730.*

EC-Council. (2009). *Computer Forensics: Hard Disk and Operating Systems, Volume 2.* Cengage Learning.

EC-Council. (2010). *Investigating Data and Image Files:.* Cengage Learning.

Elavarasi, M. (2016). Network Forensics And Its Investigation Methodology. *International Journal of Emerging Trends in Science and Technology*.

Fowler, K. (2008). *SQL server forenisc analysis.* Pearson Education.

Frauenhoffer, M. (2018). *Medium*. Retrieved August 11, 2020, from https://medium.com/@Frauenhoffer/how-to-create-a-forensic-image-with-ftk-imager-6fb8ee07fb2d

Glynn, E. A. (1984). Computer Abuse: The Emerging Crime and the Need for Legislation. *12 Fordham Urb. L.J. 73*.

Gogolin, G. (2021). *Digital Forensics Explained.* CRC Press.

Govil, J., Kaur, N., & Kaur, H. (2008). An examination of IPv4 and IPv6 networks : Constraints and various transition mechanisms. *IEEE SoutheastCon 2008*, 178-185.

Hassan, N. A. (2019). *Digital Forensics Basic.* New York: Apress.

Hayes, D. D. (2015). *A Practical Guide to Computer Forensics Investigations.* Pearson Education, Inc.

Henry, P., Williams, J., & Wright, B. (2013). The SANS Survey of Digital Forensics and Incident Response. *SANS Institute InfoSec Reading Room*.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. .* New York: Routledge.

Horsman, G., Laing, C., & Vickers, P. (2012). A case based reasoning framework for improving the trustworthiness of digital Forensic Investigations. *11th International Conference on Trust, Security and Privacy in Computing and Communications, .* IEEE.

http://sleuthkit.org/. (2012). Retrieved january sunday, 2021, from http://sleuthkit.org/autopsy/docs/user-docs/4.15.0/tree_viewer_page.html

Ironis, A. D., & Konstadopoulou, A. (2007). PROFESSIONALISM IN DIGITAL FORENSICS. *EC2ND 2006. Springer, London*.

itu.int. (2017). *itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf.* Retrieved from www.itu.int: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf

Kao, D.-Y., Wu, N.-C., & Tsai, F. (2020). A Triage Triangle Strategy for Law. *In 2020 22nd International Conference on Advanced Communication Technology (ICACT)*, 1173–1179.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* Retrieved from Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875

Kilpatrick, T., Gonzalez, J., Chandia, R., Papa, M., & Shenoi, S. (2008). Forensic analysis of SCADA systems and networks. *Int J Secur Netw 3(2)*, 95-102.

Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *SPECIAL ISSUE ARTICLE, Security and Privacy*.

Moch, C., & Freiling, F. C. (2009). The Forensic Image Generator Generator (Forensig2). *In IT Security Incident Management and IT Forensics, 2009. IMF'09, Fifth International Conference. IEEE*, 78-93.

Muneesawang, P., & Yammen, S. (2015). *Visual Inspection Technology in the Hard Disk Drive Industry.* ISTE Ltd and John Wiley & Sons, Inc.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations: Processing Digital Evidence.* 2019, 2016 Cengage Learning, Inc.

Official Journal of the European Union. (2016, 05 04). *eur-lex.europa.eu/legal-content/EN/.* Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Ogutu, J. (2016). A Methodology to Test the Richness of Forensic Evidence of Database Storage Engine: Analysis of MySQL Update Operation in InnoDB and MyISAM Storage Engines.

Olivier, M. (2009). On metadata context in database forensics. *Digital Investigation. 5(3)*, 115-123.

Palmer, G. (2001). A Road Map for Digital Forensic Research. *The Digital Forensic Research Conference.* Report From the First Digital Forensic Research Workshop (DFRWS), The MITRE Corporation.

Perry, R., Hatcher, E., Mahowald, R., & Hendrick, S. (2009). Force.com Cloud platform drives huge time to market and cost savings. *IDC*.

Pfleeger, S. L. (2015). Spider-Man, Hubris, and the Future of Security and Privacy. *IEEE Computer and Reliability Societies*.

Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis. *Digital investigation, 13*, 38-57.

Prakash, N., & Duhan, D. R. (2020). COMPUTER FORENSIC INVESTIGATION PROCESS AND JUDICIAL RESPONSE TO THE DIGITAL EVIDENCE IN INDIA IN LIGHT OF RULE OF BEST EVIDENCE. *International Journal in Management and Social Science, Volume 08, Issue 05*.

Prasanthi, B. V. (2016). Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology (IJETT) – Volume-41 Number-5* .

Provos, N., & Holz, T. (2007). *Virtual honeypots: from botnet tracking to intrusion detection.* Addison-Wesley Professional.

Ranum, M. J. (1999). *Intrusion detection and network forensics.* In USENIX Security.

Razak, S., Othman, S., Aldolah, A., & Ngadi, M. (2016). Conceptual investigation process model for managing database forensic investigation knowledge. *Res. J. Apl. Sci. Eng. Technol. 12.*, 386-394.

Rogers et. al. (2004). The future of computer forensics: a needs analysis survey. *Computer & Security, 23*, 12-16.

Salunkhe, P., Bharne, S., & Padiya, P. (2016). Data analysis of file forensic investigation. *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, 372-375.

Sammons, J. (2012). *Forensics, The Basics of Digital : the primer for getting started in digital forensics.* Syngress is an imprint of Elsevier.

Sammons, J. (2014). The basics of digital forensics: the primer for getting started in digital forensics. *Elsevier*.

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implications. *Security and Communication Neworks*.

Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis . *Journal of Digital Forensics, Security and Law: Vol. 10 : No. 2 , Article 3*.

Solodov, D., & Solodov, I. (2021). Data recovery in a case of fire-damaged Hard Disk Drives and Solid-State Drives. *Forensic Science International: Reports*.

worldbank.org. (2021, 03 19). *data.worldbank.org*. Retrieved from worldbank.org: https://data.worldbank.org/country/MK

worldbank.org. (2021, 03 19). *data.worldbank.org*. Retrieved from worldbank.org: https://data.worldbank.org/country/MK

Yannikos, Y., Graner, L., Steinebach, M., & Winter, C. (2014). Data Corpora for Digital Forensics Education and Research. *In IFIP International Conference on Digital Forensics,* (pp. 309–325). Springer.

Zakaras, M. (2001). Revue internationale de droit pénal. *International computer crimes. General report, 3(3-4),*, 813-829.

Zlatanov, N. (2015). Hard Disk Drive and Disk Encryption. *Black Hat.* Amsterdam: IEEE Computer Society.