RAQAMLI KRIMINALISTIKA VOSITALARIGA EHTIYOJLARNI BAHOLASH

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika”
Ergashbekov Nurbek Avazbek o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU

Annotatsiya: Ushbu maqolada raqamli kriminalistika tergovlarida qo‘llaniladigan apparat va dasturiy vositalar, ularning turlari, funksiyalari hamda qo‘llanish xususiyatlari yoritiladi. Raqamli kriminalistika vositalari doimiy ravishda yangilanib borayotganligi tufayli, ularning samaradorligini oshirish maqsadida yetkazib beruvchilar veb-saytlarini muntazam kuzatib borish muhimligi ta’kidlanadi. Maqolada kriminalistika vositalarini tanlash mezonlari, jismoniy va mantiqiy nusxa olish usullari, ma’lumotlarni tasdiqlash, tekshirish, filtratsiya va ekstraktsiya jarayonlari keng yoritilgan. Shuningdek, ma’lumotlarni tiklash (carving), shifrlashni ochish, kalit so‘z bo‘yicha qidiruv, ma’lumotlarni qayta qurish va hisobot yaratish kabi jarayonlar bo‘yicha amaliy yondashuvlar bayon etiladi. Xalqaro standartlar — NIST CFTT, IOCE va ISO 27037 — kriminalistika jarayonlarining ishonchliligi va izchilligini ta’minlashda asosiy ko‘rsatmalar sifatida taqdim etiladi.

Kalit so‘zlar: Raqamli kriminalistika, kriminalistika vositalari, apparat vositalari, dasturiy ta’minot, ma’lumotlarni olish, tasdiqlash, tekshirish, carving, ekstraktsiya, ma’lumotlarni tiklash, fayl tizimlari, xesh qiymatlar, NIST CFTT, ISO 27037, EnCase, FTK, X-Ways, OSForensics.

Ushbu maqolada raqamli kriminalistika tergovlarida ishlatiladigan ko‘plab dasturiy va apparat vositalari o‘rganiladi.

Raqamli kriminalistika vositalari doimiy ravishda ishlab chiqarilmoqda, yangilanmoqda. Shuning uchun, yangi funksiyalar va o‘zgarishlar uchun yetkazib beruvchilarning veb-saytlarini muntazam ravishda kuzatib turish muhimdir. Ushbu yangilanishlar hozirgi kunda duch kelayotgan muammolarni hal qilishda yordam berishi mumkin.

Har qanday kriminalistika vositasini sotib olishdan oldin, vosita tergov davomida sizga vaqt tejashini va buning tiklangan ma’lumotlarning ishonchliligiga ta’sir qiladimi-yo‘qligi ko‘rib chiqiladi. Ko‘plab grafik interfeysga ega raqamli kriminalistika vositalari ko‘p resurs, xotira va tezkor protsessorlarga ega kompyuterlarni talab qiladi. Ba’zan ular ortiqcha resurslarga ega bo‘lishi mumkin, chunki boshqa dasturlar, masalan, antivirus dasturlari, fon rejimida ishlaydi. Ushbu fon rejimidagi dasturlar raqamli kriminalistika dasturi bilan resurslar uchun Joy talashadi. Natijada raqamli kriminalistika dasturi yoki operatsion tizim to‘xtashi “qaytib qolishi” mumkin, bu esa tekshiruvlardagi kechikishlarga olib keladi.

Raqamli kriminalistika vositalariga ehtiyojlarni baholash. Raqamli kriminalistika apparat va dasturiy ta'minotni xarid qilishni asoslash uchun biznes rejasini ishlab chiqish kerak. Variantlarni o'rganayotganda, ba'zan texnik yordamni o'z ichiga oladigan ochiq manba vositalarini ko'rib chiqish mumkin. Maqsad imkon qadar ko'proq funksiyalar uchun eng yaxshi narxdagi vositani topishdir. Vositalarni tanlashda quyidagilarni inobatda olish kerak:

– Raqamli kriminalistika vositasi qaysi operatsion tizimda ishlaydi? Vosita bir nechta operatsion tizimlarda ishlay oladimi?

– Raqamli kriminalistika vositasi ko'p funksiyalimi? Masalan, u Windows va Linuxda yoki macOS da ishlaydimi?

– Raqamli kriminalistika vositasi FAT, NTFS va Ext4 kabi bir nechta fayl tizimlarini tahlil qila oladimi?

– Raqamli kriminalistika vositasi takroriy vazifalarni va ishlarni avtomatlashtirish uchun skript tili bilan ishlatilishi mumkinmi?

– Raqamli kriminalistika vositasi ma'lumotlarni tahlil qilish uchun zarur bo'lgan vaqtni kamaytirishga yordam beradigan avtomatlashtirilgan funksiyalarga egami?

– Yetkazib beruvchining mahsulot yordam berish bo'yicha obro'si qanday? Ochiq manba vositalari uchun, yordam berish forumlari qanday?

Raqamli kriminalistika vositalarining turlari. Raqamli kriminalistika vositalari ikki katta toifaga bo'linadi:

– apparat;

– dasturiy ta'minot.

Apparat turidagi raqamli kriminalistika vositalari. Apparat turidagi raqamli kriminalistika vositalari oddiy, bitta maqsadli komponentlardan to'liq kompyuter tizimlari va serverlargacha bo'lishi mumkin. Masalan, Tableau T35es-R2 SATA/IDE eSATA ko'prigi bitta qurilma yordamida SATA yoki IDE diskiga kirishni ta'minlaydigan bitta maqsadli komponentdir. Ba'zi to'liq tizimlar ya'ni, Digital Intelligence F.R.E.D tizimlari, DIBS Advanced Forensic Workstations, Forensic Computers' Forensic Examination Stations va portable units, Ace Laboratory tizimlari bo'lib, zararlangan disklar ma'lumotlarini tiklash uchun mo'ljallangan.

Dasturiy kriminalistika vositalari. Dasturiy kriminalistika vositalari buyruq satri dasturlari va grafik interfeysga ega dasturlar sifatida guruhlanadi. Ba'zi vositalar bitta vazifani bajarish uchun ixtisoslashgan. Masalan, New Technologies, Inc. (NTI) tomonidan ishlab chiqilgan SafeBack buyruq satri diskni olish vositasi sifatida mo'ljallangan. U asosiy vosita sifatida emas, balki barcha narsalar muvaffaqiyatsiz bo'lganda ishonchli zaxira sifatida ishlatiladi. Boshqa vositalar ko'plab har xil vazifalarni bajarish uchun mo'ljallangan. Masalan, PassMark Software OSForensics, X-Ways Forensics, Guidance Software EnCase, Magnet Forensics AXIOM va AccessData FTK grafik interfeysga ega vositalar bo'lib, ko'plab kriminalistika olish va tahlil funksiyalarini bajarishga mo'ljallangan.

Dasturiy kriminalistika vositalari odatda shubhali qurilmadan ma'lumotlarni tasvir fayliga nusxalash uchun ishlatiladi. Ko'plab grafik interfeysli (GUI) acquisition vositalari tasvir faylida barcha tuzilmalarni asl disk kabi o'qish va tasvir fayllarini tahlil qilish qobiliyatiga ega.

Raqamli kriminalistika vositalarining vazifalari. Barcha raqamli kriminalistika vositalari, apparat va dasturiy ta'minot, aniq funksiyalarni bajaradi. Yangi vositalarni sinab ko'rayotganda, NIST tashkilotining Kompyuter kriminalistika vositalarini sinovdan o'tkazish (CFTT) dasturi, ASTM International (ilgari Amerika Sinov va Materiallar Jamiyati) ning E2678 standartidan va Kompyuter Dalilari Xalqaro Tashkilotidan (IOCE) kelgan ko'rsatmalarga rioya qilish foydali bo'ladi. Shuningdek, ISO standarti 27037 (www.iso.org/standard/44381.html) raqamli dalil birinchi javobgarlarini (DEFR) tasdiqlangan vositalardan foydalanishni tavsiya etadi. Quyidagi funksiyalar toifalari raqamli kriminalistika vositalarini baholash uchun ko'rsatmalar sifatida xizmat qiladi, ular ma'lumotlarni tahlil qilish va tiklash shuningdek, ma'lumotlar sifatini ta'minlash uchun qo'shimcha funksiyalarni o'z ichiga oladi:

- Ma'lumotlarni olish;
- Tasdiqlash va tekshirish;
- Ekstraktsiya;
- Qayta qurish;
- Hisobot berish.

NIST tashkilotining kompyuter kriminalistika vositalarini sinovdan o'tkazish (CFTT) va boshqa guruhlarning qo'shimcha funksiyalarni, masalan, ma'lumotlarni olish, mobil qurilmalardan ma'lumotlarni chiqarish, faylni qayta qurish va satr qidirish kabi funksiyalarni o'z ichiga oladi.

Ma'lumotlarni olish. Ma'lumotlarni olish raqamli kriminalistika tergovlaridagi birinchi vazifa bo'lib, asl diskning nusxasini tayyorlashdir. Ushbu protsedura asl diskni saqlashni ta'minlaydi, shunda u buzilmaydi va raqamli dalilga zarar yetmaydi. Ma'lumotlarni olish toifasidagi qo'shimcha funksiyalar quyidagilarni o'z ichiga oladi:

- Jismoniy ma'lumot nusxasi;
- Mantiqiy ma'lumot nusxasi;
- Ma'lumot olish formati;
- Buyruq satrida olish;
- GUI orqali olish;
- Masofadan turib fizik nusxa olish.

ISO standarti 27037 ma'lumot olishdagi eng muhim omillardan biri DEFR ning kompetensiyasi hisoblanadi va tasdiqlangan vositalardan foydalanish mumkin ekanligini ta'kidlaydi va turli vaziyatlarda qanday qilib ma'lumot olishni yondashish bo'yicha ko'rsatmalarni o'z ichiga oladi. Eng muhimi, nima qilinganini va nega qilinganini hujjatlashtirishdir. Masalan, agar xavfli materiallar mavjud bo'lgan joyda ma'lumot olib qolinsa, tezlik muhim ahamiyatga ega. Shuning uchun tezkor xotirani olishni e'tiborsiz qoldirib, qurilmalarni to'plashga e'tibor qaratish mumkin. Shuningdek, butun jismoniy

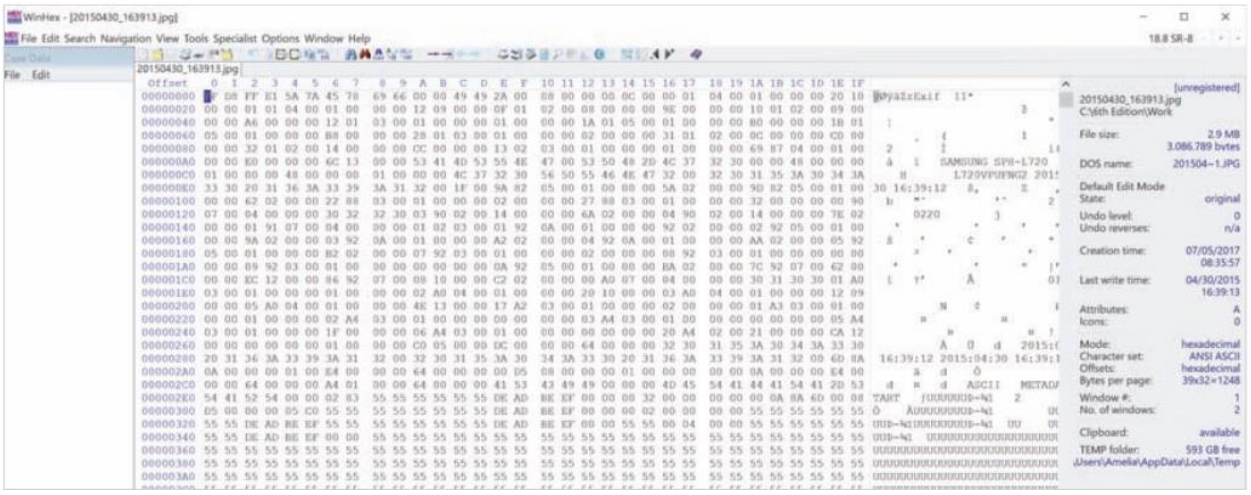
diskni nusxalash yoki faqat bir partition yoki papkaga e'tibor berish haqida qaror qabul qilish uchun oqim diagrammalarini topish kerak.

Ba'zi raqamli kriminalistika dasturiy paketlari, masalan, AccessData FTK, tasvir olish uchun alohida vositalarga ega. Masalan, Magnet AXIOM kriminalistik tasvirni olish va uni bir vaqtda qayta ishlashga imkon beradi. Biroq, ba'zi tadqiqotchilar tasvir olish uchun Tableau TD2, Logicube Talon, VOOM HardCopy 3P yoki Intelligent Computer Solutions, Inc. dan Image MASSter Solo-4 kabi raqamli kriminalistikaning apparat qurilmalaridan foydalanishni afzal ko'radilar. Ushbu apparat qurilmalari ma'lumot olish uchun o'rnatilgan dasturiy ta'minotga ega. Diskni nusxalash uchun boshqa qurilma yoki dastur kerak emas, ammo, ma'lumotlarni tahlil qilish uchun raqamli kriminalistika dasturiy ta'minoti kerak bo'ladi.

Boshqa ma'lumot olish vositalari diskni olish uchun apparat qurilmalari va dasturiy dasturlarni birlashtirishni talab qiladi. Masalan, ko'plab dasturiy vositalar disklarni faqat o'qish rejimida o'rnatadi va boshqalari jismoniy yozuvni blokirovka qilish uskunasini talab qilishi mumkin. Har qanday vosita ichida o'rnatilgan dasturiy ta'minotni blokirovka qilish vositasi mavjud bo'lsa, dalilning o'zgartirilmaganligini ta'minlash uchun uni tasdiqlash kerak.

Dasturiy ta'minot orqali nusxa olishning ikkita usuli mavjud bo'lib, ular diskning butun qismini jismoniy nusxalash va diskning partitsiyasini mantiqiy nusxalashdir. Ko'pgina dasturiy ta'minot orqali nusxa olish vositalari butun jismoniy diskni yoki faqat mantiqiy partitsiyani tasvirlash imkoniyatini o'z ichiga oladi. Odatda, vaziyat jismoniy yoki mantiqiy nusxa olishni tanlashni belgilaydi. Mantiqiy nusxa olishni tanlashning bir sababi disk shifrlanishidir.

Diskdan nusxa olish formatlari asl ma'lumotdan yetkazib beruvchi maxsus egoriyalargacha farq qiladi. Asl ma'lumot formati, odatda, Linux dd buyruqi yordamida yaratiladigan, ma'lumot faylining, disk partitsiyasining yoki butun diskning oddiy *"bit-for-bit"* nusxasidir. Asl formatli tasvir olish vositasi ma'lumotlarni bir diskdan boshqasiga yoki bo'lingan fayllarga nusxalash imkoniyatini beradi. Bu haqiqiy o'zgartirilmagan nusxa bo'lgani uchun, asl tasvir faylida mavjud bo'lgan ma'lumotni har qanday o'n oltilik ko'rinishga ega tahrirlovchi bilan ko'rish mumkin, masalan, Hex Workshop yoki WinHex misol qilsa bo'ladi. Ushbu vositalar ma'lumotlarning o'n oltilik ko'rinishini (6.1-rasmga qarang) yoki ochiq matnli ko'rinishini beradi.



1.1-rasm. WinHex dasturida ma’lumotlarni ko‘rish

Kichik segmentlangan fayllarni yaratish, ishlab chiqaruvchi sotib olish vositalarida odatiy xususiyatdir. Ularning maqsadi, olingan ma’lumotlarni kichik media, masalan, CD va USB disklariga saqlashni osonlashtirishdir.

Katta tashkilotlarda fayllardan masofadan nusxa olish keng tarqalgan. Korporativ darajadagi kompaniyalar geografik jihatdan xilma-xil bo‘lganligi sababli, tergovchilar tizimlarga jismoniy kirish uchun uzoq masofalar o‘tishi kerak bo‘lishi mumkin. AccessData va EnCase kabi mashhur vositalar tarmoqda disk tasvirlarini masofadan olish imkoniyatiga ega va bu olish jarayoni “*dd*” buyrug‘i yordamida ham amalga oshirilishi mumkin.

Tasdiqlash va tekshirish. Tasdiqlash va tekshirish funksiyalari bir-biri bilan chambarchas bog‘liq.

Tasdiqlash vositaning maqsadga muvofiq ishlayotganini tasdiqlash usuli. *Tekshirish* ikkita ma’lumot to‘plami bir xil ekanligini tasdiqlovchi jarayondir. Bu esa xesh qiymatlarini hisoblash yoki boshqa shunga o‘xshash usullar yordamida amalga oshiriladi. Boshqa bog‘liq jarayon filtratsiya, bu esa tergov natijalarini saralash va qidirish orqali yaxshi ma’lumotlarni va shubhali ma’lumotlarni ajratishni o‘z ichiga oladi. Vositalarni tasdiqlash va ma’lumotlarni tekshirish filtratsiyani amalga oshirish imkonini beradi.

Vositani tasdiqlash uchun, kompyuter va mobil qurilmalar uchun yaratilgan kriminalistik tasvirlardan foydalanish mumkin. Bu fayllar NIST tashkilotining CFTT yoki raqamli dalil bo‘yicha ilmiy ishchi guruh (SWGDE) kabi veb-saytlarda joylashtirilgan bo‘lib, ushbu vosita diskda dalil sifatida nima topishi kerakligini ko‘rsatadi. Ular natijalar chegaralarini berishi mumkin. Masalan, vosita Linux tasvirlarini olishda yaxshi ishlashini, ammo eski Windows versiyalari bilan muammolarga duch kelishini aniqlay oladi. Ushbu guruhlar, shuningdek, apparat nusxa olish vositalarini sinovdan o‘tkazish natijalarini ham chop etadi. Vositani tasdiqlagandan so‘ng, hamma kriminalistik nusxalarning bir xil xesh qiymatiga ega ekanligini ta’minlash zarur.

Barcha kriminalistika sotib olish vositalarida ma’lumot nusxalash jarayonini tekshirish usuli mavjud bo‘lib, u asl diskni tasvir bilan taqqoslaydi. Masalan, EnCase

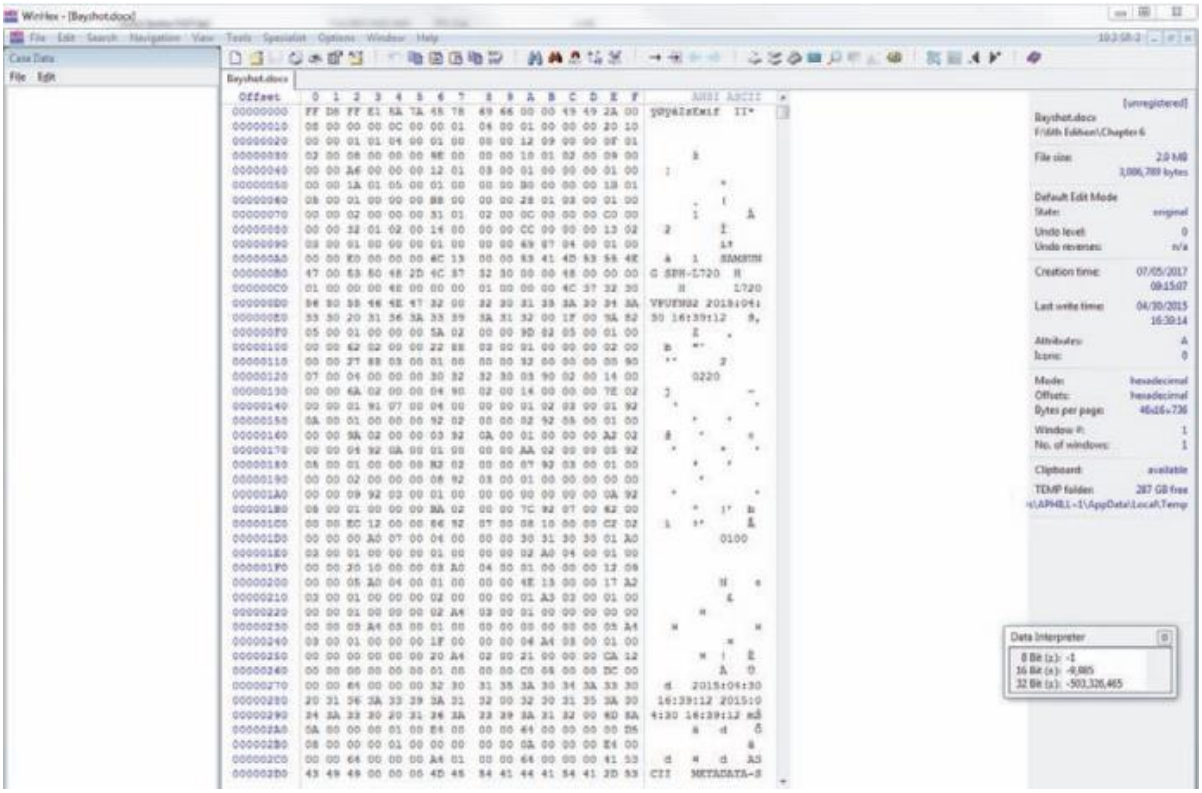
olingan ma’lumotlarning MD5 xesh qiymatini hisoblashni taklif qiladi va FTK ma’lumotlarni olish jarayonida MD5 va SHA-1 hash to‘plarini tasdiqlaydi. Image MASSter Solo-4 kabi apparat nusxa olish vositalari ma’lumot olish jarayonida bir vaqtning o‘zida MD5 va CRC-32 xeshlashni amalga oshira oladi.

Filtratsiyani amalga oshirganda, yaxshi ma’lumotlarni shubhali ma’lumotlardan ajratish kerak. Yaxshi ma’lumotlar ma’lum fayllardan iborat bo‘lib, ular operatsion tizim fayllari, umumiy dasturlar (masalan, Microsoft Word) va kompaniyaning kundalik ishlarida ishlatiladigan standart fayllarni o‘z ichiga oladi. Shuningdek, operatsion tizimning yangi o‘rnatilishi, barcha dasturlar va ma’lum yaxshi tasvirlar va hujjatlar (jadval fayllari, matn fayllari va boshqalar) uchun yaxshi xesh qiymatlari ro‘yxatini yaratish uchun ishlatish mumkin. Ushbu ma’lumotlar bilan tergovchi barcha ma’lumotlarni tanlangan yaxshi ro‘yxatga kiritmasdan, boshqa fayllarga e’tibor qaratishi mumkin. Filtratsiya shuningdek, jinoyat tergovlarida dalil uchun ma’lumotlarni topish yoki xodimni ishdan bo‘shatish, ishni qurish uchun ham qo‘llanilishi mumkin.

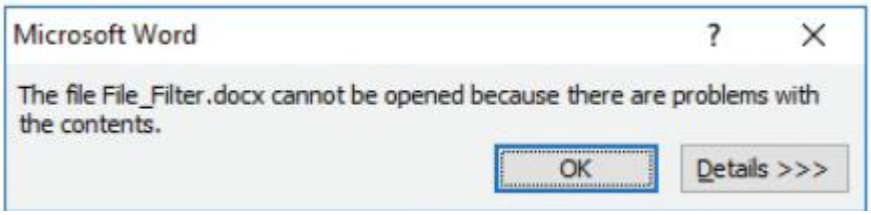
Bir nechta raqamli kriminalistika vositalari ma’lum orginal fayl xesh to‘plarini integratsiyalash va shubhali diskdan olingan fayl xesh qiymatlarini solishtirish imkoniyatiga ega. Ushbu jarayon bilan katta miqdordagi ma’lumotlarni tezda chiqarib tashlash mumkin, shunda dalil tahliliga e’tiborni qaratish mumkin. Shuningdek, o‘z xesh to‘plarini yaratishni boshlash mumkin. Yana bir muhim xususiyat ma’lumot sektorlarini xeshlash va solishtirishdadir. Bu, qisman o‘zgartirilgan bo‘lishi mumkin bo‘lgan disk joyidagi ma’lumotlar bo‘laklarini aniqlashda foydalidir.

Ma’lumotlarni filtratsiya qilishning yana bir usuli ma’lum fayl turlari uchun sarlavha qiymatlarini tahlil qilish va tasdiqlashdir. Har bir fayl turining fayl kengaytmasi bilan bog‘liq sarlavha qiymati mavjud bo‘lib, ko‘plab raqamli kriminalistika vositalari umumiy fayl sarlavhalarining ro‘yxatini o‘z ichiga oladi. Ushbu fayl sarlavhalarini ko‘rish uchun o‘n oltilik tahrirlovchisini ishlatish mumkin, bu esa fayl kengaytmasining fayl turiga mos kelmasligini aniqlash imkonini beradi. Fayl kengaytmasini o‘zgartirish ko‘pincha ma’lumotlarni yashirish yoki o‘zgartirish uchun amalga oshiriladi va agar fayl sarlavhalari tekshirilimasa, muhim ma’lumotlarni o‘tkazib yuborish mumkin. Grafik fayllar uchun standart ko‘rsatkich — “FF D8” o‘n olti lik qiymati, bu esa 6.2-rasmda ko‘rsatilgan *“Bayshot.docx”* faylining birinchi qatorida ko‘rinadi.

Bayshot.docx faylida sarlavhada “FF D8” borligi sababli, bu *.docx fayli emas *.jpeg tasviridir. Agar ushbu faylni Microsoft Word dasturida ochishga harakat qilinsa, agar Windows 7 yoki 8.1 dan foydalanilsa 6.3-rasmda ko‘rsatilgan xato xabarini ko‘rish mumkin. Biroq, Windows 10 avtomatik ravishda faylni JPEG sifatida aniqlaydi va to‘g‘ri kengaytmani qo‘shadi.

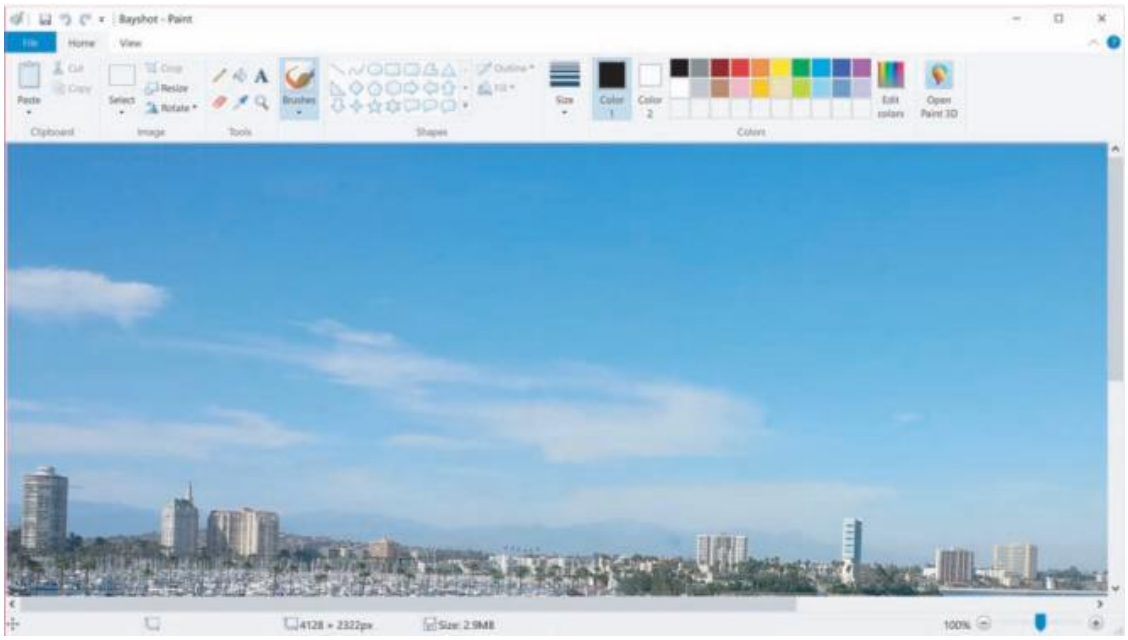


2.2-rasm. Fayl sarlavhasi *.jpeg faylini bildiradi



2.3-rasm. Word dasturida *.jpeg faylni ochishga urinayotganda xato xabari

Agar fayl Microsoft Paint kabi tasvirni ko‘rish dasturi bilan ochilsa, 2.4-rasmda ko‘rsatilgan rasmni ko‘rish mumkin.



2.4-rasm Paint dasturida “Bayshot.docx” fayli ko‘rinishi

Fayl kengaytmalari o‘rniga fayl sarlavhalarini qidirish va solishtirish filtrlashni yaxshilaydi. Ushbu xususiyat yordamida ataylab o‘zgartirilgan fayllarni topish mumkin.

XULOSA.

Raqamli kriminalistika zamonaviy tergov jarayonlarining ajralmas qismi bo‘lib, undan foydalanishda to‘g‘ri tanlangan apparat va dasturiy vositalar muhim ahamiyat kasb etadi. Vositalarni tanlashda ularning funksional imkoniyatlari, bir nechta operatsion tizimlarda ishlay olishi, fayl tizimlarini qo‘llashi, avtomatlashtirilgan funksiyalarga egaligi va texnik qo‘llab-quvvatlash xizmati mavjudligi hisobga olinadi. Ma’lumotlarni olish, tasdiqlash, tekshirish va ekstraktsiya qilish jarayonlari kriminalistik jarayonning asosiy bosqichlari bo‘lib, ular tergov uchun zarur bo‘lgan ishonchli dalillarni to‘plashni ta’minlaydi. Fayl sarlavhalari, xesh qiymatlari va carving texnikalaridan foydalanish dalillarni chuqur tahlil qilishga imkon beradi. Xalqaro standartlarga amal qilish tergov jarayonining shaffofligi va qonuniyligini ta’minlab, tergovchiga to‘g‘ri qarorlar qabul qilishga yordam beradi. Umuman olganda, raqamli kriminalistika vositalarining to‘g‘ri tanlanishi va qo‘llanishi raqamli dalillarning ishonchliligi, tahlil sifati va tergov samaradorligini oshiradi.

ADABIYOTLAR:

1. NIST — Computer Forensics Tool Testing (CFTT) Program.
2. ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence.
3. IOCE — International Organization on Computer Evidence.
4. Guidance Software — EnCase Forensic Documentation.
5. AccessData — FTK User Guide.
6. X-Ways Forensics Official Documentation.
7. Magnet Forensics — AXIOM User Manual.
8. PassMark — OSForensics Technical Specifications.
9. Brian Carrier. *File System Forensic Analysis.* Addison-Wesley.
10. Nelson, Phillips, Steuart. *Guide to Computer Forensics and Investigations.*