ИЧКИ ИШЛАР ОРГАНЛАРИ ФАОЛИЯТИДА РАҚАМЛИ КРИМИНАЛИСТИКА ВА ТЕХНОЛОГИЯЛАРНИНГ ЎРНИ ВА СУД КОМПЬЮТЕР ТЕХНИК ЭКСПЕРТИЗА ОБЪЕКТЛАРИ

Ички ишлар Вазирлиги Академияси
3-ўқув курси курсанти
Хидиров Асадбек Илҳом ўғли

Аннотация: *Данная статья посвящена цифровой криминалистике и технологиям, которые становятся наиболее актуальными в настоящее время, в ней рассказывается о новых технологиях и цифровой криминалистике.*

Ключевые слова: *история криминалистики, цифровая криминалистика, компьютерные преступления, кибератака, статистика.*

Annotation: *This article is about digital forensics and technologies, which are becoming the most relevant nowadays, it talks about new technologies and digital forensics.*

Key words: *history of forensics, digital forensics, computer crimes, cyber attack, statistics.*

Аннотация:*Ушбу мақола ҳозирги кунда энг долзарб бўлиб келаётган рақамли криминалистика ва технологиялар мавзусида бўлиб унда янги технологиялар ҳамда рақамли криминалистика тўғрисида сўз боради.*

Калит сўзлар: *криминалистика тарихи, рақамли криминалистика, компьютер жиноятлари, киберҳужум, статистика.*

Экспертиза объекти тушунчаси эксперт амалиётида асосийлардан биридир, чунки экспертизанинг айрим турларини фарқлаш ва эксперт ваколатлари чегараларини аниқлаш у билан бевосита боғликдир.СКТЭ мутахассиси томонидан ўрганилган объектлар табиий ва техник хусусиятлари, функционал мақсадлари билан ажралиб туради. Ҳозиргивақтда қуйидаги тасниф умумий қабул қилинган:

Ускуна объектлари:

- шахсий компьютерлар (стационар ва моноблоклар);
- портатив компьютерлар;
- қаттиқ магнит дисклардаги драйвлар;
- флеш-медиа;
- рақамли камералар ва видеокамералар;
- қаттиқ ҳолатдаги ҳайдовчи;
- оптик (лазер) дисклар;
- мобил қурилмалар (телефонлар, смартфонлар, планшетлар, ПДА ва бошқалар);
- СИМ-карталар;
- мобил қурилмаларда ўрнатилган хотира карталари;
- шунингдек, санаб ўтилганларга ўхшаш функцияларга эга қурилмалар.

Ахборот объектлари (маълумотлар):

-матн ва график ҳужжатлар, ишлаб чиқарилган компьютер воситаларидан фойдаланиш;

- мультимедиа форматидаги маълумотлар;

- маълумотлар базалари ва бошқа иловалар форматларидаги маълумотлар

амалий характер ва бошқалар.

Амалдаги эксперт амалиётининг таҳлили шуни кўрсатадики, рақамли экспертизага тақдим қилинадиган далилларнинг умумий рўйхатидаги энг катта улуши шахсий Компьютерлар ва ҳар хил турдаги маълумотларни сақлаш мосламалари (алоҳида ёки бошқа қурилмаларнинг бир қисми сифатида — видеорегистраторлар, рақамли камералар, GPS-навигаторлар, MP3-плеерлар ва бошқалар), мобил телефонлар ва смартфонларга тўғри келади. Кейинги қисмларда рақамли экспертиза объектлари батафсил кўриб чиқилади. Тергов пайтида компьютерлар ва унинг таркибий қисмлари қимматли далиллар бўлиши мумкин. Ускуна, дастурий таъминот, ҳужжатлар, фотосуратлар, расм файллари, электрон почта хабарлари ва қўшимчалар, маълумотлар базаси, молиявий маълумотлар, интернетга кириш тарихи, суҳбат журналлари, дўстлар рўйхати, воқеалар журналлари, ташқи қурилмаларда сақланадиган маълумотлар ва компьютер билан боғлиқ маълумотларни аниқлаш тизим ва таркибий қисмлар — буларнинг барчаси потенциал далиллардир. Компьютернинг стандарт конфигурацияси (шахсий компьютер) учта асосий функционал таркибий қисмларни ўз ичига олиши керак: 1. системали блок (микропроцессор, оператив хотира, турли хил маълумотларни сақлаш мосламаларни ўз ичига олган); 2. дисплей (монитор); 3. маълумотларни киритиш ва маълумотларни қайта ишлаш учун буйруқлар берадиган маълумотларни киритиш қурилмалари (клавиатура, турли хил манипуляторлар). Ҳозирги вақтда дунёда энг кўп ишлатиладиган шахсий компьютерларнинг икки тур архитектуралари (платформалари) мавжуд — IBMга мос келувчи компьютерлар ва Apple компьютерларидир. Шахсий компьютерлар кўчма ва стационар бўлиши мумкин. Кўчма компьютерлар барча керакли қисмларни ўз ичига олиб (шу жумладан, монитор) кичик ўлчам ва вазнга эга бўлади, Шунингдек, автоном равишда ишлаши мумкин. Ушбу турга “ноутбуклар” ва шахсий чўнтак компьютерлари киради. Ноутбук-компьютерлар (Шунингдек, “лаптоп” номи ҳам қўлланилади, инглизча laptop дан олинган — lap-ўтирган одамнинг тиззаси, laptop-тепа, юза) кўчма ўлчамда бўлиб, китоб кўринишидаги қатланадиган корпусга эга. «Ноутбукларнинг” баъзи моделларида механик клавиатура бўлмайди. Шу билан бирга, бошқариш махсус “таёқча” (“стилус”), замонавий моделларда эса — сенсорли экран ёрдамида амалга оширилади. Бундай “трансформер ноутбуклари” планшетлар режимида ҳам ишлайди, шунинг учун уларни “планшет компьютерлар” (“планшетлар”, инглизча tablet computer, tablet) билан осонгина чалкаштириб юбориш мумкин. Шу билан бирга, “планшетлар” мобил телефонлар-смартфонлар билан бир хил синфдаги платформаларда, “трансформер-ноутбуклари” эса шахсий компьютер платформасида қурилган. “Ноутбук”. Ноутбук-трансформер мисоли. Стационар шахсий компьютерлар (ёки оддий шахсий компьютерлар) одатда системали блокига интерфейс кабеллари орқали уланган монитор ва клавиатура, системали блоки каби алоҳида таркибий қисмлардан иборат бўлади. Алоҳида қурилиш схемасининг намунаси кўрсатилган.

Сўнгги пайтларда моноблокли шахсий компьютерлар кенг тарқалмоқда, бунда системали блоки, монитор ва кўпинча бошқа қурилмалар (клавиатура, овоз системаси, веб-камера, микрофон) тизимли равишда битта қурилмага бирлаштирилган. Замонавий “моноблоклар” сенсорли экран билан жиҳозланган. Компьютер технологияларининг ривожланиши билан “неттоп” деб номланган мини-компьютерлар пайдо бўлди. Неттопнинг баъзи моделларини мониторнинг орқа томонига қистириш мумкин. Шахсий компьютерлар мисоллари . “Неттоп-компьютер” мисоли. Худди шундай ҳолат электрон кўринишда тақдим этиладиган ва ўз қурилмаларида “планшетлар” га яқин бўлган электрон маълумотни намойиш қилиш учун мўлжалланган “электрон китоб” туридаги қурилмаларда (инглизча digital book, e-book reader) ҳам мавжуд. Шахсий чўнтак компьютерлар (инглизча “personal digital assistant”, PDA — “шахсий рақамли ёрдамчи”) жуда кичик ўлчамлари билан ажралиб туради. Пайдо бўлган пайтида ушбу қурилмалар кенг функционал имкониятларга эга эди. Уларнинг ёрдами билан сиз телефон орқали суҳбатлар, ёзишмалар ва воқеаларни режалаштиришингиз мумкин. Бироқ уяли технологиялар ривожланиши билан улар “смартфонлар” ва “планшетлар” билан тўлиқ алмаштирилди ва ҳозирда ишлаб чиқарилмаяпти. Хотира курилмалари. Қаттиқ дисклар, ташқи қаттиқ дисклар, олинадиган ташувчилар, флешкалар ва хотира карталари каби сақлаш мосламаларида жиноятни тергов қилишда қимматли далил бўлиши мумкин бўлган электрон почта хабарлари, кўриб чиқиш тарихи, Интернетдаги суҳбат журналлари ва дўстлар рўйхати, расмлар, расм файллари, маълумотлар базаси, молиявий ёзувлар ва воқеалар журналлари каби маълумотлар бўлиши мумкин. Электрон китоблар мисоли. Чўнтак компьютерлар. Шахсий компьютерларда маълумотларни сақлаш учун ишлатиладиган қурилмалар ташқи ва дизайн жиҳатидан жуда хилма-хилдир. Замонавий компьютер технологияларида маълумотларни сақлашнинг физик тамойилига мувофиқ магнит ёзувлар, оптик, магнитоптик ва флеш-хотирали қурилмаларга бўлинган рақамли сақлаш мосламалари қўлланилади. Магнит қурилмалар қаторига каттик магнит дискли (инглиз тилидаги hard (magnetic) disk drive, HDD, каттик диск, сленг номи — “винчестер”) ва эгилувчан магнит дискли тўплагичлар киради. Оптик асбобларга эса — CD-плеерлар. Ҳозирги пайтда флеш-дисклар алоҳида восита сифатида кенг қўлланилади ва замонавий видео ва фото камералар, уяли телефонлар ва ноутбук компьютерларида ҳам қўлланилади. “Стример” (магнит ленталар), эгилувчан магнит дискларни ўқиш мосламалари, магнит-оптик дисклар (дискеталар, магнит-оптик дисклар) каби сақлаш асбоблари (медиа) эскирган ҳисобланади ва ушбу тавсиялар доирасида кўриб чиқилмайди. Каттик магнит дискли тўплагичлари (КМДТ) ҚМДТдаги маълумотлар ферромагнит материал қатлами билан қопланган қаттиқ (алюминий ёки шиша) пластиналарга — магнит дискларга ёзилади. ҚМДТ кўпгина компьютерларда маълумотларни сақлашнинг асосий воситасидир. Компьютер технологияларида асосан икки ўлчамдаги қаттиқ дисклар (форм-фактолар) ишлатилади — 3,5 дюйм (ва ундан ихчамроқ — 2,5 дюймли. 3,5 форм-факторли ҚМДТси ва унинг қурилмаси.Ташқи ташувчиларнинг кенг тарқалган шакли — бу ҳар қандай турдаги компьютерга кабел ёрдамида уланадиган катта сиғимга эга, кичик ўлчамдаги портатив сақлаш мосламалари. Замонавий ташқи тўплагичлар симсиз уланиш (Wi-Fi) орқали маълумот алмашиш учун

бир нечта компьютерларга маълумот бериш қобилиятига эга ва уларнинг ушбу режимдаги фаолияти уларга ўрнатилган батарея билан таъминланади. . Ташқи дискларнинг намуналари (SSD, HDD).. ТАхборотни сақлаш ҳажмини, тезлигини ва ишончлилигини ошириш учун бир нечта тўплагичларни битта массивга — ташқи омборга — бирлаштириш мумкин. ашқи омборлар намунаси. Флэш-хотирали тўплагичлари. Бундай тўплагичлар кичик ўлчамларга эга ва узоқ вақт маълумотни сақлаши мумкин. Қувват манбаисиз узоқ муддат (ўн йилликлар давомида) маълумотларни сақлаш учун мўлжалланган. Рақамли камералар, чўнтак компьютерларида, смартфонлар ва бошқа қурилмаларда қўлланилади. Баъзи флеш-дисклардаги маълумотларни компьютерда ўқиш учун сизга махсус мослама («CardReader») керак бўлади. USB интерфейсига эга тўплагичлар тўғридан-тўғри компьютерга уланади. Флеш тўплагичларнинг ташқи кўриниши, ишланиши бўйича турли хил бўлишини ҳисобга олиш керак. Масалан, бундай қурилмалар билагузук, ўйинчоқ, маржон ёки калит узук ва ҳоказо шаклида ишланган бўлиши мумкин.. Турли хил флэш-хотира тўплагичлари.. Ҳар хил турдаги кўринишга эга флэш-хотира тўплагичлари. Ўрнатилган шифрлаш тизимли флеш-дисклар мавжуд бўлиб, унга кириш ҳуқуқи корпусдаги тугмачалар ёрдамида киритилган “ПИН-код” билан ҳимояланган, Шунинг дек, маълумотларга нафақат USB орқали, балки симсиз Wi-Fi орқали ҳам кириш имкониятига эга бўлган флеш-дисклар мавжуд. USB интерфейсига эга бўлган қурилмаларнинг катта қисми флеш-дискларга ўхшаш кўринишга эга. Масалан, дастурий таъминотни ҳимоя қилиш учун “электрон калитлар”, “блютуз” (инглизча bluetooth) ва “Wi-Fi” қурилмалари (адаптерлар). Ушбу турдаги қурилмалар улар тўғрисидаги маълумотларни ёзиб олиш қобилиятига эга эмас ва машина ташувчилар синфига кирмайди. Бошқа USB-қурилмаларга мисол “3G-модемлардир”. 3G-модемларнинг кўплаб моделларида олинадиган хотира картасини ўрнатиш имконияти мавжуд. Мутахассис бўлмаган кишиларга ушбу қурилмаларни (3G модемлари бундан мустасно) маркировка йўқлигида флеш-дисклардан ажратиб кўрсатиш жуда қийин. Шу сабабли, ташаббускорлар “Электрон калитлар”, “блютуз” ва “Wi-Fi” адаптерларини ахборот ташувчиси сифатида текшириш учун кўпинча тақдим. Шифрланган (а) ва Wi-Fi уланиш нуқтаси ўрнатилган (б) флеш-дисклар намуналари.. Электрон калитларнинг (а), Wi-Fi(б), блютуз адаптерлари (с) ва 3G модемлари (д) нинг ташқи кўриниши ва белгиланишига мисоллар, аммо улар ахборот ташувчиси эмас. Натижада, ушбу қурилмалар уларни идентификациялаш маълумотларини олиш учун (масалан, серия рақамлари, IMEI рақамлари) қизиқиш уйғотиши мумкин. “3G модемлар” фақатгина хотира картасига эга бўлганларида экспертиза объекти сифатида аҳамиятга эга бўлади. SSD (Каттик корпусли флеш-дисклар) Каттик корпусли тўплагич (инглизча solid-state disk, SSD) — бу флеш-хотира чиплари, контроллерлар ва уланиш интерфейси жойлашадиган плата. Турли хил интерфейсли SSD-тўплагичлар корпуссиз ҳолда ҳам ишлаб чиқарилиши мумкин.. SSD-тўплагич ва унинг ички қурилмасининг кўриниши.. Турли хил интерфейсли қаттиқ ҳолатдаги тўплагичлар.мисоллар Юқори тезлик, ориб бораётган сиғим ва ишончлилик туфайли ушбу қурилмалар янада оммалашмоқда ва келажакда шахсий компьютерлардаги магнит ёзув мосламаларини алмаштириши керак.

Оптик (лазер) дисклар. Функционал жиҳатдан оптик дисклар уч тоифага бўлинади: 1) ёзув имкониятисиз (фақат ўқиш учун, CD-ROM, DVD, BD-ROM); 2) битта ёзув ва кўп маротаба ўқиш имкониятига эга (CD-R, DVD+R, BD-R); 3) қайта ёзув имкониятига эга (CD-RW, DVD+RW, BD-RE). Биринчи тоифадаги дисклар фақат ўқиш учун мўлжалланган оз миқдордаги маълумотларни тарқатиш учун ишлатилади. Улардаги маълумотларни ўчириб ташлаш ва ёзиш мумкин эмас. Ёзув ишлаб чиқувчи заводида штамп-қурилмаларда амалга оширилади, маълумотни қайта ёзиш имкони йўқ. Шу муносабат билан, бундай дисклар деярли компьютер-техник экспертиза учун қизиқ эмас. Бироқ улар муаллифлик ҳуқуқининг бузилиши билан боғлиқ ҳолатларда олиб қўйилиши мумкин. Бир марта ёзилган дискларда маълумот тўлиқ ҳажмга еткунча бир неча марта ёзилиши мумкин (ёзиб олиш сеанслари деб аталади). Бундан ташқари, дискдаги маълумотлар сессиядан сессияга қадар фарқ қилиши мумкин ва уларнинг ҳар бирида қайд этилган маълумотни олиш мумкин. Қайта ёзиладиган дисклардан маълумотларни йўқ қилиш усулига қараб маълумотларни йўқ қилишдан кейин тиклаш мумкин. Дискларни бир-биридан белгилари орқали ажратиш мумкин. Ўқиш мосламалари, оптик дисклар ва баъзи диск белгилари.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Лех.уз (норматив ҳужжатларбазаси)
2. www.гоогле.сом (бутун жаҳон қидирув тизими)
3. эде.уз (миллий та”лим интернет портал)
4. ҳттпс://уз.wикипедиа.орг/ (Қидирув ресурслар базаси)