Informacinių technologijų ir mobiliųjų įrenginių ekspertizės

Įvadas

Informacinės technologijos, jų plėtra ir vis platesnis taikymo spektras tapo vienas ryškiausių šiuolaikinės visuomenės egzistavimo bruožų. Viena vertus, informacinių technologijų įtaka įvairioms žmonių veiklos ir gyvenimo sferoms yra akivaizdi ir naudinga; tačiau, kita vertus, jos tapo efektyviu tiek tradicinių (pvz., turto prievartavimų, pasisavinimų, sukčiavimų), tiek palyginti neseniai kriminalizuotų (pvz., neteisėtų poveikių informacinei sistemai, elektroniniams duomenims, neteisėtų prisijungimų prie informacinės sistemos) nusikalstamų veikų padarymo įrankiu. Todėl nusikalstamų veikų atskleidimo ir tyrimo praktikoje vis dažniau yra atliekami informacinių technologijų ir mobiliųjų įrenginių tyrimai (ekspertizės), kurie nustato tiriamajam įvykiui reikšmingą įrodomąją informaciją apie kompiuterinę įrangą - aparatinę įrangą, programinę įrangą, informaciją, sukauptą mobiliuose įrenginiuose ir kitose skaitmeninės informacijos laikmenose bei pačią kompiuterinę sistemą, jos funkcionavimo aplinkybes ir ypatumus.

Informacinių technologijų (IT) tyrimai Lietuvos teismo ekspertizės centre (LTEC) įdiegti nuo 1995 metų. Ekspertizių ir objektų tyrimų atlikimo Lietuvos teismo ekspertizės centre nuostatuose (toliau – Nuostatai), patvirtintuose Lietuvos Respublikos teisingumo ministro 2007-09-04 įsakymu Nr. 1R-327 (2016 m. gruodžio 9 d. įsakymo Nr.1R-311 redakcija), IT tyrimų uždaviniai yra apibrėžti taip: „Informacinių technologijų ekspertizė – nustato, atkuria, suranda duomenis, susijusius su tiriamu įvykiu, esančius kompiuterinės techninės įrangos atminties įrenginiuose; nustato stacionarios kompiuterinės techninės ir programinės įrangos veikimo aplinkybes ir vaidmenį tiriamojo įvykio atveju“. Nuo 2005 metų LTEC pradėtos mobilių įrenginių ekspertizės, kurios apibrėžtos Nuostatuose taip: “Mobiliųjų įrenginių ekspertizė − nustato, atkuria duomenis, susijusius su tiriamu įvykiu, esančius navigacijos prietaisuose, skaitmeninių stebėjimo sistemų ir garso įrašymo įrenginiuose, išmaniuosiuose ir paprastuose mobiliojo ryšio telefonuose, planšetiniuose kompiuteriuose ir kitoje įrangoje, kurioje kaupiama ir saugoma skaitmeninė informacija”. Didesnė kaip 20 metų ekspertinio darbo praktika bei sparti naujų technologijų plėtra rodo, kad atliekamų IT ir mobiliųjų įrenginių tyrimų skaičius auga, kad jie sudėtingėja, didėja tokių tyrimų objektų bazė. Šie veiksniai ir lemia būtinybę parengti metodines rekomendacijas tokių ekspertinių tyrimų užsakovams, kurios padėtų nustatyti tyrimų atlikimo LTEC galimybių ribas, išspręstų objektų pateikimo ir klausimų formavimo problemas, kylančias IT ir mobilių įrenginių tyrimų ekspertinėje praktikoje.

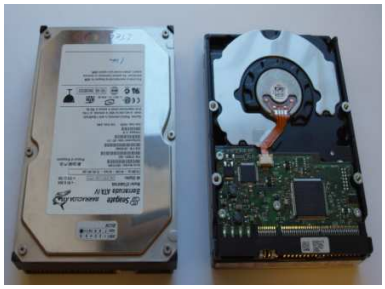
Informacinių technologijų ekspertizės objektai.

Pagrindiniai informacinių technologijų ekspertizės objektai yra įrenginiai, galintys savo atmintyje saugoti skaitmeninę informaciją. LTEC Skaitmeninės informacijos ekspertizių skyriuje

(toliau - SIES) tiriamos 1 lentelėje nurodytos pagrindinės kompiuterių skaitmeninės informacijos laikmenos. Paveikslėliuose a)-f) pateikiami skirtingų pagrindinių IT objektų pavyzdžiai.

1 lentelė: Pagrindiniai IT ekspertizės objektai.

IT ekspertizės objektas	Aprašymas
Kompiuterio sisteminis blokas (tyrimui gali būti pateikiamas su kitais kompiuterio priedais: klaviatūra, pele, maitinimo laidu ir kt.).	Kompiuterio sisteminiame bloke gali būti įmontuoti standieji diskai, įdėtos papildomos atminties kortelės, optinės laikmenos, USB atmintinės, taip pat kompiuterio sisteminio bloko atmintyje yra saugoma BIOS informacija.
Nešiojamas kompiuteris (tyrimui gali būti pateikiamas su maitinimo laidu, pele ir kt. priedais).	Nešiojamame kompiuteryje gali būti įmontuoti standieji diskai, įdėtos papildomos atminties ir SIM kortelės, optinės laikmenos, USB atmintinės, taip pat nešiojamo kompiuterio atmintyje yra saugoma BIOS informacija.
Standieji diskai (tyrimui pateikiami skirtingų tipų ir sąsajų standieji diskai).	LTEC tiriami IDE, SATA, SCSI, USB ir kitų sąsajų standieji diskai. Taip pat gali būti tiriami įvairūs išoriniai įrenginiai su naudojamais standžiųjų diskų masyvais
Papildomos atminties kortelės	LTEC tiriamos SD (mini SD, micro SD), MMC, CF ir kitų tipų atminties kortelės.
USB atmintinės.	LTEC tiriamos skirtingų dydžių ir skirtingų gamintojų USB atmintinės (laikmenos).
Optinės laikmenos.	LTEC tiriami CD, DVD diskai.

a)  b)  c) 

d)  e)  f) 

a) 3.5 colių IDE standusis diskas; b) Nešiojamasis kompiuteris; c) CD diskas; d) 2 GB talpos SD kortelė; e) Išorinis USB standusis diskas; f) Kompiuterio sisteminis blokas.

Atliekant informacinių technologijų tyrimą, gali būti pateikiami ir kiti specialūs objektai, neklasifikuoti 1 lentelėje, tačiau galintys būti tiek pagrindine, tiek ir papildoma medžiaga.

2 lentelė: Specialūs IT ekspertizės objektai.

IT ekspertizės objektas	Aprašymas
Kompiuterinės laikmenos su įrašytomis	Gali būti pateikiama tais atvejais, kai tyrimo objektų pateikti nėra galimybės arba netikslinga ar sudėtinga

tiriamųjų objektų informacijos kopijomis (pvz.: tyrimui pateikiamos duomenų bazės; programinė įranga; nukopijuota standžiųjų diskų informacija; failai su istorijos bei įvykių žurnalų įrašais ar kt.)	pateikti visą kompiuterinės įrangos komplektą, jei tyrimo objektas sudaro tik atskirai funkcionuojančią jo dalį. Pavyzdžiui, tai gali būti tiriamieji objektai su informacija iš operatoriaus serverių, teikiančių informacijos talpinimo apmokamas paslaugas ar pan.; rastos ar įtariamojo pateiktos reikiamo laikotarpio duomenų atsarginės kopijos.
Skaitmeniniai ar išspausdinti dokumentų ruošiniai ir jų kopijos, programinės įrangos, audiovizualinių kūrinių rinkmenų (failų) kopijos ir kt.	Lyginamoji medžiaga, t.y. palyginimui skirti objektai, kurių tikslių atitikmenų turi būti ieškoma tiriamuosiuose objektuose, ar nustatomos jų atsiradimo aplinkybės tiriamuosiuose objektuose.
Programinės įrangos įdiegimo failai	Pateikti reikėtų tais atvejais, jei reikia nustatyti ne programinės įrangos panaudojimo faktines aplinkybes, bet savybes: pvz., nustatyti paskirtį, veikimo mechanizmą ar principus..
IT paslaugų tiekėjo, elektroninės bankininkystės sistemų ir pan. istorijos ar įvykių žurnalų išrašai (angl. log files).	Pateikti reikėtų papildomai, jei tyrimo objektuose turi būti ieškoma konkrečių inkriminuojamos veikos požymių.

<u>Pastaba:</u> 1-2 lentelėse pateikiama IT objektų klasifikacija nėra išsami ir galutinė, ji gali keistis, nes spartus informacinių technologijų vystymasis sąlygoja vienų IT objektų išnykimą (pavyzdžiui, 3.5 colių 1.44 MB talpos lankstieji diskeliai), o kitų atsiradimą.

Be realių IT objektų, nurodytų 1-2 lentelėse, LTEC SIES yra galimybė atlikti „debesų talpyklų“ apžiūras, t.y. vartotojų elektroninio pašto, socialinių tinklų ir pan. paskyrų patikrą internete, kur gali būti saugoma tyrimui reikšminga informacija (pvz., išsaugoti susirašinėjimai žinutėmis, elektroninio pašto laiškai, atvaizdai, video ir garso įrašai bei kita galima vartotojo informacija). Tokiam „debesų“ tyrimui privalomas tyrimo užsakovo leidimas atlikti tokią apžiūrą, kartu pateikiant prisijungimo prie vartotojo paskyros (paskyrų) duomenis.

Mobiliųjų įrenginių ekspertizės objektai.

Pagrindiniai mobiliųjų įrenginių ekspertizės objektai yra mobilūs (nešiojami) įrenginiai, turintys galimybę savo atmintyje saugoti skaitmeninę informaciją. LTEC Skaitmeninės informacijos ekspertizių skyriuje (SIES) tiriami 3 lentelėje nurodyti mobilieji įrenginiai

3 lentelė: Mobiliųjų įrenginių ekspertizės objektai.

Mobiliųjų įrenginių ekspertizės objektas	**Aprašymas**
Mobiliojo ryšio telefono aparatai	Paprastų ir išmaniųjų mobiliojo ryšio telefono aparatų

(tyrimui gali būti pateikiami su SIM ir papildomos atminties kortelėmis, įkrovikliu.).	atmintyje gali būti išlikusi vartotojo ir sisteminė informacija, galimai reikšminga ar susijusi su IT tyrimo užsakovo nurodytomis aplinkybėmis bei pateiktais klausimais.
SIM kortelė (tyrimui gali būti pateikiama su dėklu).	SIM kortelės atmintyje gali būti saugomi: telefonų numerių sąrašai, SMS pranešimai, rinkti telefonų numeriai.
Planšetiniai kompiuteriai (tyrimui gali būti pateikiami su SIM ir papildomos atminties kortelėmis, įkrovikliu.)	Planšetinių kompiuterių atmintyje gali būti išlikusi vartotojo ir sisteminė informacija, galimai reikšminga ar susijusi su IT tyrimo užsakovo nurodytomis aplinkybėmis bei pateiktais klausimais.
GPS navigacijos įrenginiai (gali būti pateikiami su papildomos atminties kortelėmis, duomenų perdavimo kabeliu, įkrovikliu)	GPS navigacijų įrenginių atmintyse gali būti saugoma geografinės koordinatės, maršrutų adresai, pavadinimai.
Video įrašymo įrenginiai (angl. video recorders).	Stebėjimo kamerų užfiksuota informacija.
Garso įrašymo ir transliavimo įrenginiai (gali būti pateikiami su SIM kortele, duomenų perdavimo kabeliu).	Diktofonai, pasiklausymo įranga.
Mokėjimo kortelių skaitytuvai (angl. skimmers).	Įrenginiai galintys nuskaityti ir išsaugoti informaciją, esančią mokėjimo kortelių magnetinėse juostelėse.
Bepiločiai orlaiviai - dronai	Dronų atmintyse gali būti išlikusi vartotojo ir sisteminė informacija, galimai reikšminga ar susijusi su IT tyrimo užsakovo nurodytomis aplinkybėmis bei pateiktais klausimais.
Mobilaus ryšio (CDMA, GSM, UMTS, 3G) blokavimo įrenginiai	Gali būti nustatoma tokių įrenginių paskirtis ir galimybės.

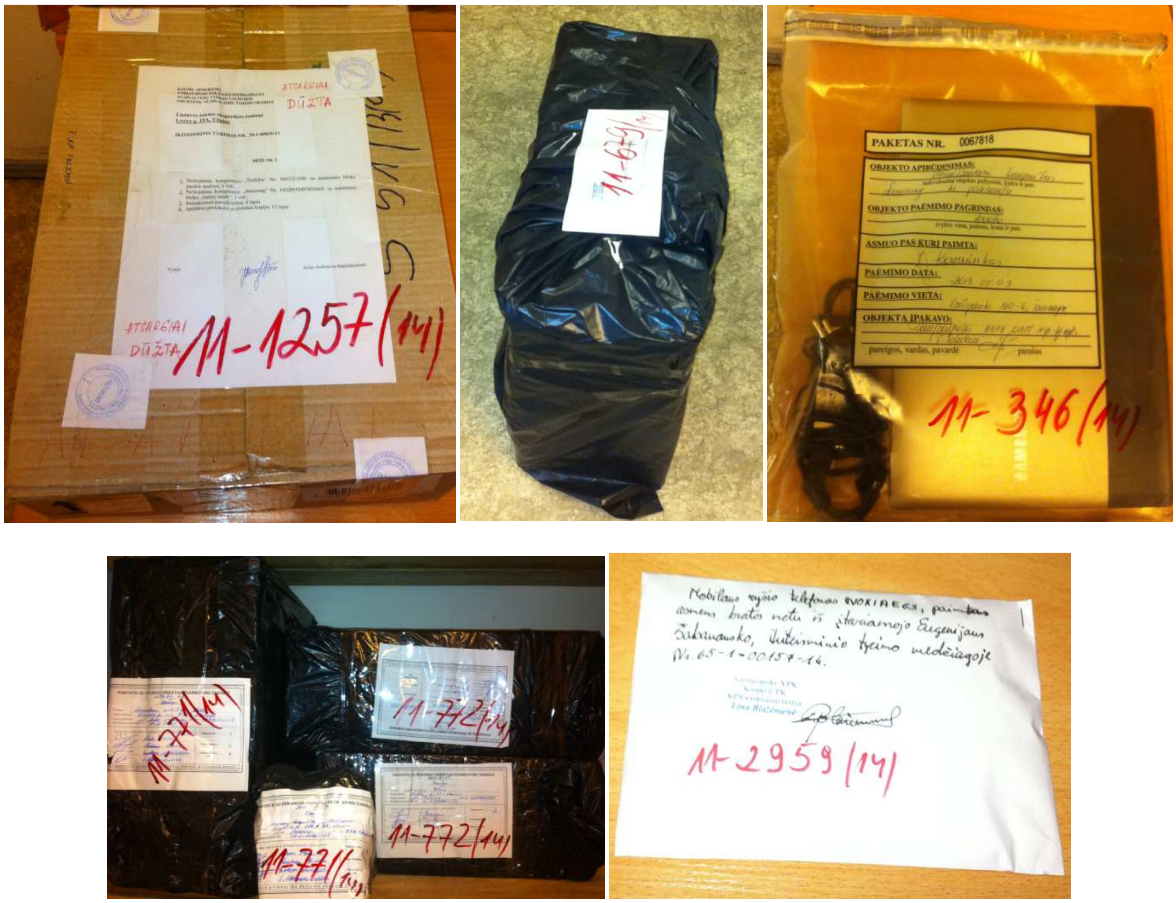
<u>Pastaba:</u> 3 lentelėje pateikiama mobiliųjų įrenginių ekspertizės objektų klasifikacija nėra išsami ir galutinė, ji gali keistis, atsižvelgiant į informacinių technologijų plėtros tendencijas.

Objektų pateikimas.

Visi tiriamieji objektai Lietuvos teismo ekspertizės centrui turi būti pateikiami supakuoti popieriniuose ar plastikiniuose paketuose (pvz.: vokuose, kartoninėse dėžėse, polietileniniuose maišuose), kurie turi būti nepažeisti, užklijuoti, tyrimo užsakovo užantspauduoti (užplombuoti). Ant kiekvieno paketo privaloma pateikti aiškiai įskaitomą informaciją:

- Pakete pateikiamų objektų pavadinimai ir tikslus vienetų skaičius. Esant galimybei papildomai pateikiama objektus identifikuojanti informacija (modelis, serijinis numeris, gamintojas ir pan.), rekomenduojama nurodyti sulaužytų (sugadintų) objektų būklę ar pažymėti fizinius defektus. Pavyzdžiui, tyrimui pateikiamas telefonas yra su įskilusiu ekranu, be maitinimo elemento (baterijos) ar nulaužta detale;

- Nurodomas ikiteisminio tyrimo, baudžiamosios bylos, civilinės bylos ar administracinės bylos numeris;
- Turi būti aiškiai ir įskaitomai užrašyta įpakavimo data bei įpakavusio asmens (ar asmenų) vardas, pavardė, parašas, pareigos.



1-5 Pav.: supakuotų objektų pavyzdžiai.

<u>Specialūs reikalavimai:</u>

- Tyrimo objektai, kuriuose gali būti išlikę drėgmės (iš vandens ištraukti ar gaisro metu gesinti įrenginiai), turi būti pakuojami popieriniuose, bet ne plastikiniuose, paketuose;
- Įjungti mobilieji įrenginiai (telefono aparatai, planšetiniai kompiuteriai) turi būti įdedami į specialius maišelius, kad būtų blokuojamas įrenginio bevielis ryšys su GSM tinklu ar kitais mobiliaisiais įrenginiais, siekiant užtikrinti šių įrenginių atmintyje vartotojo įrašytos informacijos išsaugojimą. Neturint specialaus maišelio, paprasčiausias būdas užblokuoti įrenginio bevielį ryšį yra skrydžio režimo įjungimas įrenginyje. Jeigu nėra galimybės įrenginyje nustatyti skrydžio režimą (tyrimui pateiktas įjungtas įrenginys yra apsaugotas slaptažodžiu), reikia bent jau išimti jame esančią SIM kortelę. Prieš pateikiant tyrimui veikiančius (įjungtus) objektus, užsakovas būtinai privalo susisiekti su Skaitmeninės informacijos ekspertizių skyriaus ekspertais, kad suderintų visas objekto pateikimo ir informacijos tyrimo aplinkybes bei galimybes;

- Atsakant į klausimą „Ką geriau pateikti ar visą kompiuterio sisteminį bloką ar tik jame esantį (esančius) standžiuosius diskus?“ – atsakome, kad rekomenduojama ekspertams pateikti visą kompiuterio sisteminį bloką, nes atliekant IT tyrimą, gali iškilti būtinybė ištirti įdiegtos operacinės sistemos ar aparatūrinės įrangos veikimo principus, taip pat gali būti svarbūs BIOS laiko parametrai;
- Siunčiant tyrimui nešiojamąjį kompiuterį, esant galimybei, visada rekomenduojama jį pateikti kartu su nešiojamo kompiuterio maitinimo bloku. Atliekant IT tyrimą, gali iškilti būtinybė įjungti nešiojamąjį kompiuterį.

Ekspertizės uždaviniai ir galimybės.

Standartiniai uždaviniai, atliekant IT ar mobiliųjų įrenginių ekspertinius tyrimus, yra tiriamojo objekto (įrenginio) identifikavimas, jame įrašytos informacijos kopijavimas, nukopijuotos informacijos analizė (atsižvelgiant į užduotyje (nutartyje) pateiktus klausimus) Tyrimo užsakovas užduotyje (nutartyje) atlikti tyrimą privalo nurodyti aiškius pateikiamos informacijos atrinkimo kriterijus, remdamasis faktiškai nustatytomis įvykio aplinkybėmis ir tyrimo metu surinkta reikšminga informacija. Apibendrinant galima išskirti keturis IT ir mobilių įrenginių ekspertizių pagrindinius atlikimo etapus:

1) Tyrimui pateiktų objektų identifikavimas;
2) Tyrimui pateiktų objektų informacijos nuskaitymas (kopijavimas);
3) Nuskaitytos informacijos analizė;
4) Paieškos rezultatų sisteminimas ir pateikimas užsakovui.

Objektų identifikavimas. LTEC SIES tiriami skirtingos paskirties įrenginiai: kompiuterių sisteminiai blokai, nešiojamieji kompiuteriai, mobiliojo ryšio telefonai (MRT), standieji diskai, vaizdo stebėjimo sistemos įrenginiai (DVR įrenginiai), GPS imtuvai ir kiti, savo atmintyje skaitmeninę informaciją saugantys, įrenginiai (žr. 1 ir 3 lenteles). Atlikus tyrimui pateiktų objektų pirminę apžiūrą, visi šie įrenginiai identifikuojami, t.y. gali būti. nustatomas įrenginio tipas, modelis, gamintojas, veikimo principai, būklė. Apžiūros metu nustatoma, ar įrenginys yra veikiantis, ar galima su LTEC SIES turima programine ir aparatūrine įranga nuskaityti įrenginio atminties skaitmeninę informaciją. Galimi atvejai, kai tyrimui pateikiami įrenginiai (pavyzdžiui garso transliavimo, mobilaus ryšio blokavimo įrenginiai) nesaugo savyje vartotojo informacijos, arba pateikiami sugadinti, sudegę ar savadarbiai įrenginiai, kuriuos SIES ekspertai atskirais atvejais taip pat gali identifikuoti, nustatyti šių įrenginių paskirtį, veikimo principą ir panaudojimo galimybes.

Skaitmeninės informacijos kopijavimas. LTEC informacinių technologijų ekspertai atlikdami IT standartinių objektų (žr. 1 lentelę) tyrimą, siekiant išvengti tyrimui pateikto įrenginio atmintyje vartotojo įrašytos informacijos sugadinimo (pakeitimo), informacijos kopijavimo metu naudoja blokavimo įrenginius, kurių pagalba kopijuoja informaciją ir tolesnius tyrimus atlieka su

identiškomis informacijos kopijomis. Išimtinais atvejais, kai, naudojant blokatorių, nėra galimybės nukopijuoti duomenis, informacija gali būti kopijuojama kitais metodais, kuriems būtinas įrenginio (kompiuterio) įjungimas. Tokiu atveju įrenginio įjungimas gali lemti informacijos įrenginyje (kompiuteryje) pasikeitimus, kurie dažniausiai tiriamajai informacijai įtakos neturi.

Pastaba: LTEC ekspertai, nustatę, kad įrenginio (kompiuterio) įjungimas (užkraunant tiriamoje laikmenoje esančią operacinę sistemą) yra neišvengiamas, įrenginį įjungia tik gavę tyrimo užsakovo leidimą.

Nuskaitant informaciją iš mobiliųjų įrenginių (žr. 3 lentelę) atminčių, dažniausiai šių įrenginių įjungimas yra būtinas, kartu su juose saugomos sisteminės informacijos pakeitimu (konfigūravimu). Ekspertinė praktika rodo, kad, atliekant tokių įrenginių informacijos nuskaitymą, yra nedidelė tikimybė, kad įrenginyje esanti vartotojo informacija gali būti prarasta. Pagrindinės priežastys – fizinis ar programinis įrenginio gedimas. Taip pat vartotojo informacija (dažniausiai mobiliojo ryšio telefonuose) gali būti prarandama siekiant panaikinti ar apeiti įrenginio apsaugą. Dėl minėtos priežasties LTEC ekspertai, įvertinę galimybę apeiti (panaikinti) telefono apsaugą ir nuskaityti informaciją, kreipiasi į tyrimo užsakovą dėl leidimo taikyti vieną ar kitą metodą ir perspėja apie galimas pasekmes, kurios gali lemti tiriamosios informacijos praradimą.

Rekomendacija: tyrimo užsakovai, žinodami, kad jų siunčiami mobiliojo ryšio telefonai yra apsaugoti slaptažodžiais, įvertinę neišvengiamą informacijos nuskaitymo riziką, užduotyje atlikti objektų tyrimą iš karto gali suteikti ekspertams leidimą atlikti reikalingus šių įrenginių tyrimus. Sutikimo teksto pavyzdys užduotyje atlikti objektų tyrimą, galėtų būti: sutinku ir leidžiu LTEC ekspertams su turima specialia programine ir aparatine įranga panaikinti (apeiti) tyrimui pateikto mobiliojo ryšio telefono apsaugą.

Nesant tyrimui pateikto įrenginio atminties informacijos nuskaitymo galimybės (pvz., LTEC neturi tinkamos programinės ir aparatinės įrangos), apžiūros metu ekspertas gali užfiksuoti ir pateikti užsakovui tik įrenginyje matomą, bet su specialiomis priemonėmis nenuskaitytą, reikalingą informaciją. Minėtas metodas gali būti taikomas tiriant mobiliuosius įrenginius (MRT aparatus, GPS navigacijas).

Informacijos analizė. LTEC atliekamų IT tyrimų sudėtingumui ir jų atlikimo laikui turi įtakos pateikto objekto nuskaitytos informacijos analizė. Labai svarbu, kad tyrimo užsakovai užduotyje (nutartyje) kuo tiksliau nurodytų įvykio aplinkybes, užduotų aiškius, tinkamai suformuluotus, konkrečius klausimus ekspertui, nes tai gali ženkliai įtakoti atliekamo IT tyrimo trukmę. Dažniausiai IT ekspertų prašoma tyrimui pateiktuose objektuose (laikmenose) surasti išlikusią informaciją, kuri yra susijusi su užsakovo vykdomu tyrimu ir ją pateikti užsakovui. Tokių tyrimų pavyzdžiai yra:

- Dokumentų ruošinių ar jų atvaizdų, video įrašų, atvaizdų, siųstų ar gautų elektroninių laiškų bei kitų failų paieška pagal bylų (failų) plėtinius, failų antraštes, nurodytus tekstų fragmentus;
- Informacijos paieška pagal nurodytus raktinius žodžius. Jei tyrimo užsakovas informacijos paieškai pats nurodo raktinius žodžius, jie turi būti išskirtiniai, specifiniai, su tyrimu ar nustatytomis aplinkybėmis susiję pavadinimai, žodžiai, vardai, slapyvardžiai, frazės ar pan. Privalu vengti

bendrinių žodžių ir pavadinimų, dažnai pasitaikančių bendrinėje kalboje ar internete, nes tai negali užtikrinti teigiamų paieškos rezultatų;

- Bendravimo realiu laiku internete programų informacijos tyrimas, vartotojų bendravimo istorijos ar išrašų pateikimas;
- Interneto naršyklių informacijos tyrimas, vartotojo internete lankytų puslapių sąrašo pateikimas, vartotojo vykdytų paieškų ar atliktų elektroninių pirkimų, tyrimas;
- Buhalterinės apskaitos programų tyrimas, išlikusių buhalterinių duomenų pateikimas, neatliekant buhalterinės minėtų programų funkcijų bei duomenų interpretacijos (nes tai nėra IT ekspertų kompetencijoje).

Priklausomai nuo tiriamuosiuose objektuose saugomos informacijos ekspertai gali atsakyti į papildomai pateikiamus klausimus, susijusius su:

- Rastos informacijos sukūrimo, turinio keitimo datomis ir laiku;
- Kompiuterių internetinio tinklo parametrais ir nustatymais
- Kompiuterių operacinių sistemų parametrais ir nustatymais.
- Kitų kompiuteriuose įdiegtų programų veikimo principais.

Atliekant mobiliųjų įrenginių tyrimus, dažniausiai ekspertų prašoma surasti, ištirti ir pateikti 4 lentelėje išvardintą informaciją:

4 lentelė: Skaitmeninė informacija, kuri gali būti saugoma mobiliųjų įrenginių atmintyse.

Bendroji informacija	Įrenginio serijos numeris, laiko ir datos nustatymai, modelis, apsaugos kodas.
Adresų knyga	Vartotojo telefonų knyga.
Ryšiai	Vartotojo priimtų, praleistų, rinktų telefonų sąrašai.
Pranešimai	Trumposios SMS žinutės, daugialypės MMS žinutės, e-laiškai, e- pokalbiai.
Kalendorius	Užduotys, užrašai, priminimai.
Vietos	GPS koordinatės, lankyti adresai.
Žiniatinklis	Lankyti (naršyti) puslapiai internete, internetinių puslapių adresai.
Atvaizdai	Paveikslėliai, nuotraukos.
Garso įrašai	Vartotojo įrašyti, sukurti garso įrašai.
Vaizdo įrašai	Vartotojo įrašyti, sukurti video įrašai.
Sisteminiai failai	Dokumentai, archyvai, rinkmenos, įvykių žurnalas.
Ištrinta informacija	Ryšiai, pranešimai, atvaizdai, video ir garso įrašai (jų fragmentai).

Rastų rezultatų sisteminimas ir pateikimas užsakovui. Atlikę objektų tyrimą ir informacijos analizę, LTEC ekspertai tyrimo rezultatus įrašo į optines laikmenas (CD ar DVD diskus) ir informaciją pateikia užsakovui kaip priedą prie specialisto išvados (ekspertizės akto). Išimtinais atvejais, kai pateikiamos informacijos kiekis yra nedidelis, ekspertai gali ją pateikti išspausdintą.

<u>Pastaba:</u> Jei su specialisto išvada pateikiamos informacijos kiekis yra didesnis negu 4 standartiniai DVD-R diskai (apie 18 GB), tyrimo užsakovų prašoma pateikti papildomą skaitmeninės informacijos laikmeną, kurios talpa atitiktų rastos (iškeliamos) informacijos talpą.

Užduoties (nutarties) ruošimas ir klausimų formulavimas

Bendrieji reikalavimai nutarties, užduoties įforminimui, medžiagos pateikimui yra išdėstyti Nuostatų V ir VI skyriuose,

Lietuvos Respublikos Generalinio prokuroro 2011-01-18 įsakymu Nr. I-14 patvirtintose „Rekomendacijose dėl užduočių specialistams ir ekspertams skyrimo tvarkos“[1], nurodyti informacinių technologijų ekspertinių tyrimų skyrimo ypatumai:

„82. Prieš skiriant informacinių technologijų tyrimą būtina nuspręsti, kokia informacija, galimai esanti kompiuterinėse laikmenose, yra būtina:

82.1. išsamiam nusikalstamos veikos atskleidimui;

82.2. nusikalstamos veikos kvalifikavimui;

82.3. konkrečioms byloje įrodinėtinoms aplinkybėms nustatyti.

83. Užduotyje formuluojami klausimai turi sietis su šių Rekomendacijų 82 punkte nurodytos informacijos gavimu ir turi sietis su konkrečios bylos aplinkybėmis.“

Taip pat šiose rekomendacijose yra aiškiai apibrėžti ir veiksniai lemiantys ekspertizių atlikimo trukmę: “ Objektų tyrimų ir ekspertizių greitam atlikimui didelės įtakos turi:

4.1. Objektų tyrimų ir ekspertizių skyrimo faktinių pagrindų pagrįstumas;

4.2. Tinkamas ikiteisminio tyrimo bylose esančių duomenų įvertinimas ir tinkamas klausimų formulavimas;

4.3.Greitas medžiagos, reikalingos objektų tyrimui ar ekspertizei atlikti, pateikimas;

4.4. Specialistų ar ekspertų bendravimas su pareigūnais objektų tyrimo, ekspertizės metu;“

LTEC SIES praktika rodo, kad tinkamas užduoties „Atlikti informacinių technologijų tyrimą“ parengimas ir klausimų formulavimas yra ypač svarbūs veiksniai, lemiantys atliekamo IT tyrimo terminus, spartą ir kokybę.

Užduoties rengimas. Tyrimo užsakovas, skirdamas informacinių technologijų ekspertinį tyrimą, turi pateikti visą IT tyrimui galimai reikšmingą turimą ar tyrimo metu nustatytą informaciją,

[1] Valstybės žinios, 2011-01-20, Nr. 8-379

pvz.,: kokie kompiuteriai (įrenginiai), kada, kur, iš kokio vartotojo buvo paimti; konkrečiai apibūdinta vykdyta nusikalstama veika; apklausos metu nustatyti ar įtariamųjų asmenų pateikti kompiuterių vartotojų, mobiliųjų įrenginių slaptažodžiai, SIM kortelių PIN kodai ar pan. informacija. Tais atvejais, kai reikia atlikti informacijos paiešką ar atkurti informaciją, pavyzdžiui, rasti dokumento ruošinį, rekomenduojama kartu pateikti ir ieškomo dokumento išspausdintą kopiją. Neturint kopijos ar žinant tik dokumento pavadinimą, svarbu pateikti kuo tikslesnius galimų raktažodžių pavyzdžius, kurie palengvintų vykdomą paiešką. Būna atvejų, kai tyrimo užsakovai patys atlieka pirminę tiriamosios laikmenos informacijos apžiūrą, o po to skiria ekspertinį tyrimą. Tokiais atvejais kartu su pavedimu atlikti tyrimą būtina pateikti atliktos pirminės apžiūros protokolo kopiją, su informacija, kada buvo jungiamas kompiuteris, kas buvo žiūrėta, kokie veiksmai buvo atliekami su tyrimo objektais ir kas nustatyta.

Spręstinų klausimų suderinimas ir papildomos informacijos pateikimas. Jeigu prieš tyrimą ar tyrimo eigoje IT specialistas nustato, jo požiūriu, tolesniam tyrimui reikšmingus dalykus ar aplinkybes, leidžiančias iš esmės susiaurinti ar praplėsti spręstinų klausimų ratą, tuomet, susisiekus su tyrimo užsakovu, abipusiu susitarimu klausimai gali būti patikslinti, išplėsti ar pakeisti. Jeigu IT tyrimai dar nepradėti arba jau vykdomi, ir paaiškėja naujos tyrimui reikšmingos aplinkybės, atsiranda naujos tiriamosios medžiagos ar užsakovui kyla papildomų klausimų, arba iškelti klausimai tampa neaktualūs, pageidautina, kad pirminiai klausimai būtų atšaukti, o papildomi klausimai pateikti kuo anksčiau, nes tai leistų IT užduoties užsakovui ir vykdytojui sutaupyti užduoties atlikimo laiką, sąnaudas bei pagerinti tyrimo rezultatų kokybę.

Klausimų formulavimas. Klausimai turėtų būti suformuluoti tiksliai, konkrečiai ir aiškiai. Jie turi būti reikšmingi ir atitikti ikiteisminio tyrimo medžiagą, sietis su bylos aplinkybėmis ir byloje tiriamu laikotarpiu,. Klausimų eiliškumas turi būti nuoseklus ir logiškas. Rekomenduojama vengti bendro pobūdžio, nekonkrečių arba perteklinių klausimų bei klausimų, nereikalaujančių specialių ekspertinių žinių, bet susijusių su didelio kiekio informacijos peržiūra ar skaitymu.

Rekomenduojami klausimų pavyzdžiai :

Nr.	Klausimas
1.	Ar tyrimui pateiktuose objektuose yra išlikę "SKYPE" ir kitų, bendrauti internete skirtų, programų elektroniniai susirašinėjimai bei elektroniniai laiškai su šiais asmenimis: Vardenis Pavardenis1, Vardenis Pavardenis2 ....?
2.	Ar tyrimui pateiktame kompiuterio sisteminiame bloke yra išlikusi informacija apie laikotarpyje nuo 2018-09-14 iki 2018-09-21 sukurtus (keistus) dokumentus, susijusius su UAB „Pavyzdys“(kopija pridedama prie užduoties)? Jei taip – prašome iškelti ir atstatyti minimus dokumentus bei nurodyti jų sukūrimo (keitimo) datas.
3.	Ar kompiuteryje yra informacijos, dokumentų, susijusių su UAB „Pavyzdys 1“, įm. kodas – 000000000; UAB „Pavyzdys 2“, įm. k. – 000000000 UAB, bei su asmeniu – Vardenis Pavardenis, asm. kodas – 30000000000. **Atkreiptinas dėmesys į tai, kad bylai reikšmingi dokumentai ar dokumentų ruošiniai yra tik tie, kuriuose išskirtinai yra paminėtas ar nurodytas asmuo – Vardenis Pavardenis**, kuris yra (ar buvo) visų aukščiau išvardintų įmonių fiktyvus direktorius.
4.	Ar tyrimui pateiktame nešiojamo kompiuterio standžiajame diske yra išlikusios informacijos apie jungimąsi prie interneto, ar yra techniniai įrenginiai, leidžiantys naudotis

	internetu laisvės atėmimo vietoje?
5.	Ar tyrimui pateiktame kompiuteryje yra išlikusios informacijos, susijusios su 2019-01-01 atliktomis finansinėmis operacijomis, naudojant elektroninę bankininkystę (žinomi sąskaitų numeriai Nr. LTXX XXXX XXXX XXXX XXXX, Nr. LTXX XXXX XXXX XXXX XXXX, Nr. LTXX XXXX XXXX XXXX XXXX, Nr. LTXX XXXX XXXX XXXX XXXX)?
6.	Ar tyrimui pateiktame kompiuteryje yra išlikusios informacijos apie Vardenis Pavardenis, a.k. xxxxxxxxxxx, asmens duomenis, bankines sąskaitas, ir pan.?
7.	Ar tyrimui pateiktame kompiuteryje yra išlikusios informacijos, susijusios su nuo 2019-01-01 iki 2019-01-02 laikotarpiu atliktomis finansinėmis operacijomis, paimant greitus kreditus iš UAB „Credit.24“; UAB „VIA SMS LT“; UAB „Nordecum“? Ar yra išlikusios informacijos apie apsilankymą šių bendrovių internetinėse svetainėse?
8.	Ar tyrimui pateiktame nešiojamame kompiuteryje yra išsaugoti failai, kuriuose būtų užfiksuoti duomenys apie siuntą Nr. XXXXXXXXXXXX iš Nyderlandų, t.y. informaciją, susijusią su narkotinių bei psichotropinių medžiagų ieškojimu, užsakymu, mokėjimu ir siuntimu Vardenis Pavardenis vardu į Lietuvos pašto Vilniaus centriniame pašte esančią pašto dėžutę Nr. XXXX Vilnius CP, LT01005?
9.	Ar elektroninio pašto susirašinėjimo istorijoje yra duomenų apie narkotinių medžiagų pirkimą (iš Nyderlandų Karalystės ar kitų šalių), jų vartojimą ir pan., taip pat ir kitą informaciją, susijusią su siunta Nr. XXXXXXXXXXXX iš Nyderlandų?
10.	Ar pateiktose kompiuterinėse laikmenose yra UAB „Pavyzdys1“ ir UAB „Pavyzdys2“ statybos rangos 2018-01-26 sutartis Nr. XX-XX, koks jos sudarymo kompiuterinėje laikmenoje laikas, tekstas?
11.	Ar tyrimui pateiktuose objektuose (kompiuteriuose, USB laikmenose) yra informacijos, galimai susijusios su UAB „Pavyzdys“ buhalterine apskaita ir kitų dokumentų, susijusių su šia įmone? Jeigu taip, tai visus dokumentus susijusius su minėta UAB „Pavyzdys“ prašome įrašyti ir pateikti į atskirą laikmeną.
12.	Ar tyrimui pateiktuose trijuose kompiuteriuose yra pasų, asmens tapatybės kortelių, vairuotojų pažymėjimų ir kitų dokumentų ruošinių?
13.	Ar tyrimui pateiktame kompiuterio sisteminio bloko kietajame diske ir kompaktiniame diske yra 50 eurų banknotų Nr. XXXXXXXXX ar kitų pinigų banknotų ruošinių ?
14.	Ar tyrimui pateiktų kompiuterių standžiuose diskuose yra failų (video, nuotraukų), kuriuose yra pavaizduoti galimai nepilnamečiai asmenys su apnuogintais lytiniais organais, bei lytiniai santykiai, kurių dalyviai yra galimai nepilnamečiai asmenys?
15.	Kokia informacija (adresatai – kontaktai, trumposios SMS žinutės, ryšiai (rinkti, gauti, praleisti)) yra išlikusi tyrimui pateiktame telefone „NOKIA“ (IMEI 000000/04/000000/0) ir „labas“ SIM kortelėje Nr. 89370000000000000000?
16.	Ar pateiktame tyrimui mobilaus ryšio telefone „Samsung Galaxy S6“ ir jo atminties kortelėje yra ištrintas vaizdo įrašas ir nuotraukos susiję su tiriamu įvykiu?
17.	Ar mobiliojo ryšio telefone „Samsung“ yra išsaugotos trumposios SMS žinutės? Jei taip, prašome pateikti trumpąsias SMS žinutes atskiroje laikmenoje.
18.	Kokie įrašai yra išlikę pateiktuose mobiliojo ryšio telefonų bei juose esančių SIM kortelių telefonų knygose?
19.	Ar pateiktoje tyrimui navigacijoje yra išlikusi informacija apie 2019-01-01 iki 2019-03-19 vykimo maršrutus, tiek Lietuvoje tiek užsienyje?
20.	Ar pateiktame GPS imtuve yra išsaugoti duomenys su maršrutais, koordinatėmis, jei taip prašome jas pateikti, taip pat nustatyti jų datas ir laikus?

<u>Pastaba</u>. Jeigu IT tyrimo užsakovui kyla neaiškumų ar abejonių dėl klausimų formulavimo, siekiant išvengti perteklinių, specialisto kompetencijai nepriskirtinų klausimų, ar klausimų, nepagristai išplečiančių tyrimo (ekspertizės) apimtis ir laiką, klausimų formuluotes rekomenduojama iš anksto aptarti ar patikslinti su LTEC IT ekspertais (specialistais).

Apžiūra ir greitoji linija

Apžiūra. LTEC yra susidariusi atliekamų informacinių technologijų ir mobiliųjų įrenginių tyrimų eilė, todėl LTEC pagrindinėje savo būstinėje Vilniuje ir Klaipėdos skyriuje yra įkūrusi specialias apžiūros vietas, kuriose užsakovai su eksperto pagalba gali greičiau peržiūrėti ir išrinkti galimai tyrimui reikšmingą informaciją. Norint užsakyti apžiūrą, susisiekiama su ekspertais ir aptariamos galimybės bei paskiriamas apžiūros laikas. Tokiu atveju ekspertams (specialistams) yra pateikiamas vienintelis klausimas(prašymas):

<u>Prašau pateikti visų failų esančių tyrimui pateiktos laikmenos atmintyje sąrašą.</u>

Atlikus apžiūrą klausimas yra tikslinamas:

<u>Prašau pateikti ikiteisminiam tyrimui Nr.X-XXXX-19 galimai reikšmingą informaciją (reikšmingus failus), esančią tyrimui pateiktoje laikmenoje.</u>

<u>Pastaba:</u> apžiūra atliekama tik dalyvaujant tyrimo užsakovui, kuris gali nurodyti tyrimui reikšmingą informaciją.

Greitoji Linija. Tais atvejais, kai užsakovai nori spartesnių rezultatų ir patys gali savarankiškai atlikti informacijos analizę ar peržiūrą, skiriant tyrimą LTEC ekspertams duodama užduotis padaryti tyrimui pateiktų laikmenų kopijas (informacijos išrašus), įrašant jas į užsakovų pateikiamą papildomą laikmeną, bet neatliekant informacijos analizės. Toks informacijos kopijavimas (informacijos išrašų sukūrimas), priklausomai nuo tyrimui pateiktų objektų tipo, kiekio ir apimties, LTEC atliekamas pagreitintai ir užtrunka 1-4 mėn. Žemiau pateikiami klausimų pavyzdžiai, kuriuos turėtų užduoti užsakovas, norėdamas gauti laikmenos informacijos kopiją arba išrašą.

Tik kopijos arba informacijos išrašų pateikimo klausimų formulavimo pavyzdžiai.

1) Prašome padaryti tyrimui pateiktame objekte (pateiktuose objektuose) esančios informacijos identišką kopiją (Šis klausimas turi būti užduodamas objektams išvardintiems 1 lentelėje).

2) Prašome pateikti visą informaciją esančią tyrimui pateiktame objekte (pateiktuose objektuose), kurią galima nuskaityti su LTEC turima specialia programine ir aparatūrine įranga. (Šis klausimas turi būti užduodamas objektams išvardintiems 3 lentelėje).

3) Prašome padaryti tyrimui pateiktuose objektuose esančios informacijos susijusios su (pasirinktinai: adresų knyga, ryšiais, GPS koordinatėmis, SMS žinutėmis, e-laiškais, internetinių pokalbių programų istorija, atvaizdais, vaizdo įrašais, dokumentų ruošiniais) išrašą (išrašus). (Šis klausimas turi būti užduodamas įrenginiams išvardintiems 1, 3 lentelėse).