UDHËZUES PËR HETIMIN E KRIMIT KOMPJUTERIK

OSCE Organizata për Siguri dhe Bashkëpunim në Evropë
Prezenca në Shqipëri

UDHËZUES PËR HETIMIN E KRIMIT KOMPJUTERIK

Tiranë, 2022

UDHËZUES PËR HETIMIN E KRIMIT KOMPJUTERIK

Tiranë, 2022

Autor: Marjan Stoilkovski
Konsulent Ndërkombëtar

Organizata për Siguri dhe Bashkëpunim në Evropë
Prezenca në Shqipëri

PËRMBAJTJA

Ky dokument fokusohet në mënyrën se si zbatohen parimet e përcaktuara në legjislacion për përdorimin e internetit, duke përfshirë mediat sociale, si një mjet hetimor.

Çdo veprimtari duhet të shqyrtohet rast pas rasti, në përputhje me politikat e Policisë dhe Prokurorisë dhe me legjislacionin kombëtar për angazhimin e hetimit, komunikimin dhe përdorimin e teknologjisë.

Disa nga udhëzimet mbulojnë fusha të teknikave të fshehta hetimore që mund të prekin të drejtat e një personi dhe që duhet të përdoren vetëm kur është e nevojshme dhe në mënyrë proporcionale. Legjislacioni shqiptar për mbikëqyrjen dhe mbrojtjen e të dhënave siguron kuadrin për të garantuar që një veprim i tillë është i ligjshëm dhe në përputhje me Konventën Evropiane të të Drejtave të Njeriut (KEDNj).

Ky dokument është objekt rishikimi dhe ndryshimeve të vazhdueshme për të marrë parasysh zhvillimet në legjislacion, teknologji, efektet e proceseve të gjykimit dhe çështjet e trajtuara..

HYRJE

Ky dokument synon të shpjegojë krimet kompjuterike dhe të ofrojë këshillim për hetimet paraprake, që nga marrja e ankesës fillestare për një krim deri në pikën kur hartohen planet përgatitore për të arrestuar një të dyshuar dhe/apo për të sekuestruar media digjitale, si dhe shtjellon trajtimin për hetimet paraprake.

Në rastet e krimeve kompjuterike në ditët e sotme, të marrurit me një pajisje digjitale apo një hetim digjital ndodh përditë, pasi pjesa dërrmuese e njerëzve kanë një pajisje elektronike/digjitale, nga të cilat më të njohurat janë telefonat celularë, tabletat dhe laptop-ët; me rritjen e përdorimit të e-mail dhe mediave sociale, shumica e ankesave për krime do të përfshijnë analizimin dhe të kuptuarit e këtyre medieve dhe fushave të mundshme që do të ndihmojnë hetimet

Në pamje të parë, kjo teknologji mund të duket e ndërlikuar, por zyrat e prokurorisë dhe efektivët e policisë janë përshtatur me përhapjen e telefonave celularë dhe kanë njohuri se si komunikojnë pajisjet, si dhe faktin që kompanitë e telekomunikacionit mbajnë regjistrime për mbajtësit e llogarive dhe të dhënat identifikuese të telefonave, të tilla si numri IMEI, të dhënat e kartave SIM, numrin e alokuar të telefonit, regjistrime të përdorimit dhe mënyrat e pagesës.

Synohet që po këto elemente të thjeshtohen kur bëhet fjalë për kompjuterat, Internetit, web-in dhe mediat sociale, duke dhënë një link për legjislacionin për krimet kompjuterike, një hyrje në terminologjinë e kompjuterave dhe rrjetave dhe shpjegim për funksionin e saj, si dhe, ç'është më e rëndësishmja, se çfarë informacioni ka të ngjarë t'ju ndihmojë gjatë shqyrtimeve të ankesave për krime kompjuterike, si dhe se kush mund t'ju ndihmojë gjatë një hetimi.

Fushat e veçanta që do të mbulohen janë legjislacioni përkatës për hetimet e krimeve kompjuterike:

- Ligji nr. 7895, datë 27.01.1995, Kodi Penal i Republikës së Shqipërisë, i ndryshuar (me Ligjet nr. 43/2021 dhe 89/2017)
- Ligji nr. 7905, datë 21.03.1995, Kodi i Procedurës Penale i Republikës së Shqipërisë, i ndryshuar (me Ligjin nr. 41/2021)
- Ligji nr. 9918, datë 19.05.2008, "Për komunikimet elektronike", i ndryshuar
- Ligji nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale", i ndryshuar
- Ligji nr. 9880, datë 25.02.2008, "Për nënshkrimin elektronik", i ndryshuar

KAPACITETET KOMBËTARE PËR HETIMIN E KRIMEVE KOMPJUTERIKE

Me rritjen e krimeve kompjuterike dhe përdorimin e pajisjeve elektronike/digjitale nga kriminelët në vepra penale, gjithnjë e më shumë të dhëna dhe prova gjenden të ruajtura në format elektronik. Për të përballuar këtë mjedis në ndryshim, Drejtoria e Policisë në Shqipëri ka investuar në krijimin e njësive të specializuara për të luftuar krimin kompjuterik dhe në zhvillimin e aftësive të efektivëve për të ndërmarrë dhe ndihmuar në hetime penale që përfshijnë përdorimin e mediave elektronike/digjitale dhe krimeve që lidhen me kompjuterat.

Për momentin, ekzistojnë dy njësi të specializuara për krimet kompjuterike; më poshtë renditen rolet dhe përgjegjësitë e tyre të tanishme, bashkë me hollësi se si ata mund t'u japin asistencë prokurorëve me këshilla në lidhje me ankesat fillestare për krimet dhe me hetimet penale, që nga sigurimi i të dhënave në media elektronike/digjitale, apo si të kryejnë kërkime dhe hetime të sigurta në Internet.

Njësia e Hetimit të Krimeve Kompjuterike

Njësia e Hetimit të Krimeve Kompjuterike e ka qendrën në Tiranë dhe mban përgjegjësi kombëtare për hetimin e krimeve kompjuterike si vijon:

- Përdorimin e paautorizuar të pajisjeve kompjuterike;
- Sulmet me programe keqdashëse, Hyrjet e paautorizuara;
- Shpërdorimin e Rrjeteve;
- Mbrojtjen e të Dhënave Personale;
- Imazhet e pahijshme të fëmijëve;
- Mashtrimet me bankomatët;
- Mashtrimet me pagesat elektronike;
- Mashtrimet me kartat e kreditit/debitit;
- Leximin e fshehtë të kartave;
- Bashkëpunimin rajonal dhe ndërkombëtar;
- Bashkëpunimin me bankat dhe institucionet financiare;
- Bashkëpunimin me Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Në plotësimin e misionit të saj dhe për t'i dhënë prokurorisë mbështetje efikase në hetimin e krimeve kompjuterike dhe mbledhjen e provave digjitale, Njësia e Hetimit të Krimeve Kompjuterike mund të zhvillojë kapacitete dhe t'u kushtojë vëmendje një sërë veprimtarive shtesë, përfshirë edhe në vijim:

- Planifikimin paraprak të një hetimi që ka lidhje me krime kompjuterike të ndërlikuara;
- Gjetjen e të Dhënave në Kohë Reale apo të të Dhënave të Paqëndrueshme;
- Kërkimin e informacionit mbi rrjete pa tel (wireless) apo që ndodhet në to;
- Këshillat se si të mblidhen të dhëna komunikimi nga partnerët kombëtarë apo ndërkombëtarë (Kërkesa për Arkivim të Dhënash);
- Hetimet mbi të Dhëna Komunikimi – Email-e, Media Sociale, adresa IP, ofruesit e shërbimeve telefonike dhe të Internetit;
- Këshillat mbi Mbledhjen e të Dhënave nga Burime të Hapura (Open Source Intelligence / OSINT) – Realizimi i kërkimeve mbi pajisjet dhe sigurinë operacionale gjatë kërkimeve në Media Sociale, Dhoma Chat-i, IRC, kërkimi në linjë për të dyshuar apo dëshmitarë;
- Kërkimet e Fshehta për Mbledhje të Dhënash nga Burime të Hapura;
- Incidentet që prekin Infrastrukturën Kritike Kombëtare të Shqipërisë;

LEGJISLACIONI PËR KRIMET KOMPJUTERIKE

Konventa e Budapestit për Krimet Kompjuterike

Konventa mbi krimet kompjuterike konsiderohet si marrëveshja ndërkombëtare më përkatëse mbi krimin kompjuterik dhe provat elektronike. Konventa e Budapestit përgjithësisht jep rekomandime në fushat e:

- kriminalizimit të sjelljes, duke nisur nga hyrja e paligjshme, ndërhyrja në të dhëna dhe sisteme, deri te mashtrimet me bazë kompjuterike dhe pornografia e fëmijëve;
- mjeteve ligjore proceduriale për të hetuar krimin kompjuterik dhe për të siguruar prova elektronike në lidhje me çfarëdo krim;
- bashkëpunimit efikas ndërkombëtar.

Konventa e Budapestit është një dokument ligjor që parashikon kriminalizimin e krimit kompjuterik, pushtetet proceduriale për sigurimin e provave elektronike dhe bazë ligjore për bashkëpunim ndërkombëtar. Implementimi i konventës mbi krimin kompjuterik do të sigurojë ndikim në nivel kombëtar mbi:

- legjislacionin e brendshëm mbi krimin kompjuterik dhe provat elektronike në botë;
- hetimet e brendshme të mbështetura mbi këtë legjislacion;
- bashkëpunimin ndërkombëtar, edhe për rastet serioze dhe të organizuara të krimit kompjuterik;
- bashkëpunimin publik/privat;
- forcimin e kapaciteteve të drejtësisë penale.

Konventa mbi krimin kompjuterik pajton vizionin e një Interneti të lirë, ku informacioni mund të lëvizë lirisht, si dhe të qaset dhe të shpërndahet lirisht, me nevojën për një përgjigje efektive të drejtësisë penale në rastet e shpërdorimit kriminal.

Kodi Penal

Neni 192/b – Hyrja e paautorizuar kompjuterike

Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

Neni 293/a – Përgjimi i paligjshëm i të dhënave kompjuterike

Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

Neni 293/b – Ndërhyrja në të dhënat kompjuterike

Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet. Kur kjo vepër kryhet në të dhënat kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

Neni 293/c – Ndërhyrja në sistemet kompjuterike

Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.

Neni 293/ç – Keqpërdorimi i pajisjeve

Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik

ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenet 192/b, 293/a, 293/b e 293/c të këtij Kodi, dënohen me burgim nga gjashtë muaj deri në pesë vjet.

Neni 186/a – Falsifikimi kompjuterik

Futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet. Kur kjo vepër kryhet nga personi, që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike, në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda për interesin publik, dënohet me burgim tre deri në dhjetë vjet.

Neni 143/b – Mashtrimi kompjuterik

Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet. Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.

Neni 117 – Pornografia

Prodhimi, shpërndarja, reklamimi, importimi, shitja e botimi i materialeve pornografike në mjediset ku ka fëmijë, me çdo mjet ose formë, përbëjnë kundërvajtje penale dhe dënohen me burgim deri në dy vjet. Prodhimi, importimi, ofrimi, vënia në dispozicion, shpërndarja, transmetimi, përdorimi ose posedimi i pornografisë së fëmijëve, si dhe krijimi i aksesit në mënyrë të vetëdijshme në të, me çdo mjet ose formë, dënohet me burgim nga tre deri në dhjetë vjet. Rekrutimi, përdorimi, shtrëngimi, ose bindja e një fëmije, për të marrë pjesë në shfaqje pornografike, ose marrja pjesë në shfaqje pornografike që përfshijnë fëmijët, dënohet me burgim nga pesë deri në dhjetë vjet.

Neni 23 i Kodit Penal – Përgjegjësia për tentativën

Personi që tenton të kryejë një krim përgjigjet për të. Gjykata, në varësi të shkallës së afërsisë së pasojës, si dhe të shkaqeve për të cilat krimi mbeti në tentativë, zbut dënimin dhe mund ta ulë atë nën minimumin e parashikuar nga ligji ose të caktojë një lloj dënimi më të butë nga ai i parashikuar në ligj.

Neni 27 i Kodit Penal – Përgjegjësia e bashkëpunëtorëve

Organizatorët, shtytësit dhe ndihmësit kanë përgjegjësi si edhe ekzekutorët për

veprën penale të kryer prej tyre. Në caktimin e dënimit për bashkëpunëtorët, gjykata duhet të mbajë parasysh shkallën e pjesëmarrjes së secilit dhe rolin e luajtur në kryerjen e veprës penale.

Kodi i Procedurës Penale

Neni 221 i Kodit të Procedurës Penale – Kufijtë e lejimit

1. Përgjimi i komunikimeve të një personi ose të një numri telefoni me telefon, faks, kompjuter ose me mjete të tjera të çdo lloji, përgjimi i fshehtë me mjete teknike i bisedave në vende private, përgjimi me audio dhe video në vende private dhe regjistrimi i numrave të telefonit, hyrës dhe dalës, lejohen vetëm kur procedohet:
   - për krimet e kryera me dashje, për të cilat parashikohet dënim me burgim jo më pak, në maksimum, se shtatë vjet;
   - për kundërvajtjet penale të fyerjes e të kanosjes, të kryera me mjete të komunikimit.

Neni 222 i Kodit të Procedurës Penale - Vendimi për lejimin e përgjimit

1. Me kërkesën e prokurorit, për rastet e lejuara në paragrafin 1, të nenit 221, gjykata autorizon përgjimin me vendim të arsyetuar, kur ai është i domosdoshëm për vazhdimin e hetimeve të filluara dhe kur në ngarkim të personit ekziston një dyshim i arsyeshëm dhe i bazuar në prova se ka kryer një vepër penale.
2. Kur ka arsye të bazuara për të menduar se nga vonesa mund t'i vijë një dëm i rëndë hetimeve dhe plotësohen kushtet e paragrafit 1, të këtij neni, prokurori vendos përgjimin me akt të motivuar dhe njofton gjykatën menjëherë, por jo më vonë se njëzet e katër orë nga marrja e vendimit. Kur vleftësimi nuk bëhet në afatin e caktuar, përgjimi nuk mund të vazhdojë dhe rezultatet e tij nuk mund të përdoren.
3. Kur njëri nga dy personat që do të përgjohen është i gatshëm të kryejë dhe të regjistrojë veprimin përkatës, sipas marrëveshjes me oficerin e policisë gjyqësore, veprimi lejohet me autorizim të prokurorit.
4. Në rastet e parashikuara në paragrafët 1, 2 dhe 3, të këtij neni, gjykata merr vendim të arsyetuar në dhomë këshillimi, brenda 24 orëve nga paraqitja e kërkesës së prokurorit. Kundër vendimit që refuzon kërkesën për përgjim mund të bëhet ankim i veçantë në gjykatën e apelit brenda 24 orëve. Gjykata e apelit shqyrton ankimin brenda 48 orëve nga marrja e akteve. Paraqitja e

kërkesës për vleftësimin e përgjimit nuk shkakton ndërprerjen e tij.

5. Vendimi për përgjimin tregon mënyrën e kryerjes dhe kohëzgjatjen e veprimeve, e cila nuk mund t'i kalojë pesëmbëdhjetë ditët. Ky afat, me kërkesë të arsyetuar të prokurorit, mund të zgjatet nga gjykata sa herë është e nevojshme, për një periudhë prej 15 ditësh, kur ekzistojnë kushtet e parashikuara në paragrafin 1, të këtij neni, dhe rezultatet e përgjimit diktojnë nevojën e zgjatjes së afatit.

6. Në vendimin e gjykatës për përgjimin e fshehtë, fotografik ose me video, ose për përgjimin e bisedave në vende private mund të autorizohet oficeri i policisë gjyqësore ose specialisti i kualifikuar për të hyrë në këto vende, në mënyrë të fshehtë, duke vepruar në përputhje me vendimin. Ky autorizim duhet të zbatohet brenda 15 ditëve.

7. Në regjistrin që mbahet në prokurori shënohen aktet që urdhërojnë, autorizojnë, vleftësojnë ose zgjasin përgjimet, si dhe fillimin e mbarimin e veprimeve të çdo përgjimi.

8. Në rastet e parashikuara nga neni 221, paragrafi 2, veprimi autorizohet nga prokurori.

Neni 299/a - Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike

1. Prokurori mund të urdhërojë ruajtjen e përshpejtuar të të dhënave kompjuterike të caktuara, duke përfshirë të dhënat e trafikut, kur ka shkaqe të mjaftueshme për të besuar se të dhënat mund të humbasin, dëmtohen ose ndryshohen.

2. Në rastin kur të dhënat kompjuterike janë në zotërim ose në kontroll të një personi, prokurori mund ta urdhërojë këtë person t'i ruajë dhe t'i mirëmbajë këto të dhëna kompjuterike, për një periudhë deri në 90 ditë, me qëllim zbulimin dhe nxjerrjen e tyre. Ky afat, për shkaqe të arsyeshme, mund të zgjatet vetëm një herë.

3. Personi i ngarkuar për ruajtjen dhe mirëmbajtjen e të dhënave kompjuterike detyrohet të mbajë sekret procedurat dhe veprimet e kryera, sipas pikës 2 të këtij neni, deri në përfundim të hetimeve.

Neni 299/b - Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike

Personi i ngarkuar me ruajtjen e përshpejtuar të të dhënave të trafikut detyrohet të marrë të gjitha masat e nevojshme, për të garantuar se të dhënat e ruajtura janë të vlefshme, pavarësisht nëse një apo më tepër dhënës shërbimesh kanë qenë të përfshirë në transmetimin e komunikimit,

si dhe t'i sigurojë prokurorisë ose oficerit të policisë gjyqësore, të autorizuar, zbulimin e një sasie të mjaftueshme të të dhënave të trafikut, në mënyrë që të mundësohet identifikimi i dhënësit të shërbimit dhe shtegu, nëpërmjet të cilit komunikimi është transmetuar.

Neni 191/a - Detyrimi për paraqitjen e të dhënave kompjuterike

1. Gjykata, në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, me kërkesë të prokurorit ose viktimës akuzuese urdhëron mbajtësin ose kontrolluesin të dorëzojnë të dhënat kompjuterike të memorizuara në një sistem kompjuterik apo në një mjet tjetër memorizimi.

2. Gjykata, në këto procedime, urdhëron edhe dhënësin e shërbimit për dorëzimin e çdo informacioni për abonentët e pajtuar, për shërbimet e ofruara nga dhënësi.

3. Kur ka arsye të bazuara për të menduar se nga vonesa mund t'u vijë një dëm i rëndë hetimeve, prokurori vendos, me akt të motivuar, detyrimin për paraqitjen e të dhënave kompjuterike, të përcaktuara në pikat 1 e 2 të këtij neni dhe njofton menjëherë gjykatën. Gjykata vlerëson vendimin e prokurorit brenda 48 orëve nga njoftimi.

Neni 208/a - Sekuestrimi i të dhënave kompjuterike

1. Në rastin e procedimeve për krime që lidhen me teknologjinë e informacionit, gjykata, me kërkesën e prokurorit, urdhëron sekuestrimin e të dhënave ose sistemeve kompjuterike. Në këtë vendim gjykata përcakton të drejtën për të hyrë, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimin për kryerjen e veprimeve të mëtejshme apo sigurimin e të dhënave ose të sistemit kompjuterik.

2. Kur ekzistojnë shkaqe të arsyeshme për të menduar se të dhënat e kërkuara kompjuterike janë memorizuar në një sistem tjetër kompjuterik apo në një pjesë të tij dhe këto të dhëna janë në mënyrë të ligjshme të kapshme prej ose janë të disponueshme nga sistemi kompjuterik fillestar, që kontrollohet, gjykata, me kërkesë të prokurorit, urdhëron menjëherë kërkimin ose hyrjen edhe në këtë sistem kompjuterik.

3. Në zbatim të vendimit të gjykatës, prokuroria ose oficeri i policisë gjyqësore, i deleguar nga prokurori, merr masa:

   - për të ndaluar kryerjen e veprimeve të mëtejshme ose për të siguruar sistemin kompjuterik, vetëm të një pjese të tij ose të një mjeti tjetër memorizimi të dhënash;
   - për të nxjerrë dhe marrë kopje të të dhënave kompjuterike;

- për të penguar hyrjen në të dhënat kompjuterike, ose për t'i hequr këto të dhëna nga sistemet kompjuterike me të drejtë hyrjeje;
- për të siguruar paprekshmërinë e të dhënave përkatëse, të memorizuara.

4. Për zbatimin e këtyre veprimeve, prokurori mund të urdhërojë thirrjen e një eksperti, i cili ka njohuri rreth funksionimit të sistemeve kompjuterike apo të masave të zbatuara për mbrojtjen e të dhënave kompjuterike në të. Eksperti i thirrur nuk mund të refuzojë detyrën pa shkaqe të arsyeshme.

Ligje të tjera kombëtare përkatëse

Ligji nr. 9918, datë 19.05.2008 "Për komunikimet elektronike"

Neni 101 "Ruajtja dhe administrimi i të dhënave për qëllime të ndjekjes penale"

1. Pavarësisht përcaktimeve të tjera në këtë ligj, sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve elektronike publike detyrohen të ruajnë dhe të administrojnë, për një afat 2-vjeçar, skedarët e të dhënave për pajtimtarët e tyre.
2. Skedarët duhet të përmbajnë të dhëna në lidhje me komunikimin zanor dhe me SMS/MMS, që mundësojnë:
   - identifikimin e pajtimtarëve, duke siguruar marrjen dhe regjistrimin e identitetit të plotë të tyre;
   - identifikimin e pajisjes fundore, të përdorur gjatë komunikimeve;
   - përcaktimin e vendndodhjes, datës, kohës, kohëzgjatjes së komunikimit dhe numrit të thirrur dhe thirrës, përfshirë të dhënat për thirrjet pa përgjigje.
3. Këta skedarë duhet t'u vihen në dispozicion pa vonesë, edhe në formë elektronike, autoriteteve që përcakton Kodi i Procedurës Penale, në bazë të kërkesës së tyre.

Legjislacioni për Krimet Kompjuterike në Shqipëri trajtohet nga këto ligje:

- Ligji nr. 7895, datë 27.01.1995, Kodi Penal i Republikës së Shqipërisë, i ndryshuar (me Ligjin nr. 43/2021 dhe 89/2017)
- Ligji nr. 7905, datë 21.03.1995, Kodi i Procedurës Penale i Republikës së Shqipërisë, i ndryshuar (me Ligjin nr. 41/2021)
- Ligji nr. 9918, datë 19.05.2008, "Për komunikimet elektronike", i ndryshuar
- Ligji nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale", i ndryshuar
- Ligji nr. 9880, datë 25.02.2008, "Për nënshkrimin elektronik", i ndryshuar

Kodi Penal rendit shkeljet që vijojnë:

- Neni 74/a Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 11)
- Neni 84/a Kanosja me motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 12)
- Neni 117 /2 Pornografia (Shtuar paragrafi i dytë me ligjin nr. 9859, datë 21.1.2008; ndryshuar me ligjin nr. 144, datë 2.5.2013, neni 29)
- Neni 119/a Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 13)
- Neni 119/b Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 13)
- Neni 137/a Vjedhja e rrjetit të komunikimeve elektronike (Shtuar paragrafi i parë me ligjin nr. 8733, datë 24.1.2001; ndryshuar paragrafi i dytë me ligjin nr. 10 023, datë 27.11.2008; ndryshuar me ligjin nr. 98/2014, datë 31.7.2014)
- Neni 143/b Mashtrimi kompjuterik (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 15; shfuqizuar pjesa që parashikon edhe dënimin me gjobë, si dënim kryesor, krahas dënimit me burgim, me ligjin nr. 144, datë 2.5.2013, neni 48)
- Neni 186/a Falsifikimi kompjuterik (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 18)
- Neni 192/b Hyrja e paautorizuar kompjuterike (Shtuar me ligjin nr. 8733,

neni 53; ndryshuar me ligjin nr. 9686, datë 26.2.2007; nr. 10 023, datë 27.11.2008, neni 19)

- Neni 293/a Përgjimi i paligjshëm i të dhënave kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 23)
- Neni 287 Pastrimi i produkteve të veprës penale ose veprimtarisë kriminale
- Neni 293/b Ndërhyrja në të dhënat kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 23; shtuar paragrafi i tretë me ligjin nr. 36/2017, datë 30.3.2017)
- Neni 293/c Ndërhyrja në sistemet kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 23; shtuar paragrafi i tretë me ligjin nr. 36/2017, datë 30.3.2017)
- Neni 293/ç Keqpërdorimi i pajisjeve (Shtuar me ligjin nr. 10 023, datë 27.11.2008, neni 23)

Procedurat për hetimet dhe sekuestrimin e provave elektronike mbulohen nga Kodi i Procedurës Penale në nenet që vijojnë:

- Neni 299/a i Kodit të Procedurës Penale (KPP) - Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike (Shtuar me ligjin nr. 10 054, datë 29.12.2008, neni 4)
- Neni 101 i ligjit nr. 9918, datë 19.05.2008 "Për komunikimet elektronike" - Ruajtja dhe administrimi i të dhënave për qëllime të ndjekjes penale
- Neni 299/b i KPP - Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike (Shtuar me ligjin nr. 10 054, datë 29.12.2008, neni 4)
- Neni 191/a i KPP - Detyrimi për paraqitjen e të dhënave kompjuterike (Shtuar me ligjin nr.10 054, datë 29.12.2008, neni 2)
- Neni 208/a i KPP - Sekuestrimi i të dhënave kompjuterike (Shtuar me ligjin nr.10 054, datë 29.12.2008, neni 3; ndryshuar pika 1 me ligjin nr. 35/2017, datë 30.3.2017, neni 112)
- Nenet 221-223 e KPP – Përgjimi i komunikimeve (përfshirë dispozitat për kufijtë, autorizimet dhe procedurat) (Shtuar me ligjin nr.9187, datë 12.2.2004, neni 2, neni 3, neni 4 dhe neni 5; shtuar me ligjin nr. 35/2017, datë 30.3.2017, neni 117, neni 118, neni 119, neni 120)
- Neni 15 (1) i Ligjit nr. 9918, datë 19.05.2008 "Për komunikimet elektronike" përcakton se, në autorizimin e përgjithshëm, Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) mund të përfshijë kushte lidhur me: "f) lejimin e përgjimit nga autoritetet kompetente, të përcaktuara në legjislacionin në fuqi për përgjimin e telekomunikimeve dhe zbatimin e detyrimeve, që burojnë nga ky legjislacion".

Legjislacioni në Shqipëri përcakton mbrojtjet në vijim

Kushtetuta e Republikës së Shqipërisë deklaron se të drejtat dhe liritë themelore të njeriut janë të pandashme, të patjetërsueshme e të padhunueshme dhe qëndrojnë në themel të të gjithë rendit juridik. Ajo kërkon gjithashtu që organet e pushtetit publik, në përmbushje të detyrave të tyre, duhet të respektojnë të drejtat dhe liritë themelore të njeriut, si dhe të kontribuojnë në realizimin e tyre. Për më shumë, neni 17 i Kushtetutës përcakton se çdo kufizim i të drejtave dhe lirive mund të vendoset vetëm me ligj, për një interes publik ose për mbrojtjen e të drejtave të të tjerëve dhe duhet të jetë në përpjesëtim me gjendjen që e ka diktuar atë. Kufizimet nuk mund të cenojnë thelbin e lirive dhe të të drejtave dhe në asnjë rast nuk mund të tejkalojnë kufizimet e parashikuara në Konventën Evropiane për të Drejtat e Njeriut.

Kushtetuta garanton, midis të tjerash:

Neni 22 - Lirinë e shprehjes

Neni 23 - Të drejtën për informim

Neni 36 - Lirinë dhe fshehtësinë e korrespondencës ose të çdo mjeti tjetër të komunikimit

Neni 37 - Paprekshmërinë e banesës

Disa mbrojtje shtesë sigurohen nga KPP, Ligji Për Mbrojtjen e të Dhënave, Ligji Për të Drejtat dhe Mbrojtjen e Fëmijës. Kodi i Sjelljes "Për përdorimin e sigurtë dhe të përgjegjshëm të rrjeteve dhe shërbimeve të komunikimeve elektronike në Shqipëri" u nënshkrua ndërmjet operatorëve shqiptarë në datën 07.02.2013 (https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Dokumenti%20i%20Politikave%20per%20Sigurine%20Kibernetike%202015-2017.pdf).

Si rregull, legjislacioni kombëtar përcakton kushtin e mbikëqyrjes juridike, konkretisht kërkimin e autorizimit nga një gjyqtar për masa të caktuara proceduriale nëse rrezikohen të drejtat themelore (për shembull, në rastet e përgjimit të komunikimeve apo për mbledhjen e të dhënave të trafikut).

Përveçse në shkelje penale kompjuterike, pajisjet elektronike/digjitale mund të përdoren edhe në kryerjen e shumë veprave të tjera penale, dhe në të dyja rastet është me rëndësi që të përcaktohet lidhja e pajisjes me të dyshuarin dhe veprimin penal. Ky dokument për të informuar dhe ballafaqon këtë tip hetimi digjital me një hyrje në teorinë dhe udhëzimet në fushat përkatëse, për të përfshirë:

- Identifikuesit e pajisjeve
- Serverat

- Adresat IP
- Email-et
- Interneti
- World Wide Web (www.)
- Ruajtja dhe Mbledhja e të Dhënave
- Partneritetet
- Mbledhja e të Dhënave nga Burime të Hapura (Open Source Intelligence – OSINT)
- Siguria kibernetike
- Shfrytëzimi i të miturve në Internet

Për secilën nga këto fusha subjekt do të ketë një shënim në fund të faqes për të dhënë disa fjalë kyç që lidhin me seksionin përkatës.

BURIMET E PROVAVE ELEKTRONIKE

Përdorimi i provave elektronike është rritur në vitet e fundit pasi gjykatave u është dashur të pranojnë dhe marrin në konsideratë prova elektronike në formën e e-mail-eve, fotografive digjitale, regjistrave të transaksioneve në ATM, dokumenteve të përpunimit të tekstit, mesazheve të çastit, fletëllogaritjeve, historive të shfletuesit të internetit, bazave të të dhënave, përmbajtjes së kujtesës së kompjuterit, kopjeve rezervë të kompjuterit, printimeve kompjuterike dhe skedarëve me video dhe audio digjitale – të gjitha këto përbëjnë të dhëna digjitale.

Një pajisje digjitale e përfshirë në krim duhet të sigurohet njësoj siç do të bënit me format e tjera të provave fizike të gjetura në një vendngjarje krimi, sepse të gjitha pajisjet e tilla mbeten prova fizike. Ashtu si me gjurmët e gishtërinjve dhe provat e ADN-së, provat digjitale janë të brishta dhe humbasin ose ndryshohen lehtësisht nëse nuk ndiqen masat e duhura të kujdesit paraprak.

Është e rëndësishme të regjistrohet se ku është gjetur dhe sekuestruar pajisja digjitale, pasi kjo mund të zbulojë shumë për qëllimin e autorit të dyshuar. Është praktikë e mirë regjistrimi me video i kontrollit dhe sekuestrimit. Kjo do të tregojë vendndodhjen e pajisjeve digjitale, në mënyrë që të mos ketë më një argument, për shembull, nëse pajisja me valë u gjet e fshehur në papafingo dhe jo në një zonë të hapur në dhomën e ndenjes.

Provat elektronike gjenden zakonisht në sistemet kompjuterike. Sistemet kompjuterike mund të paraqiten në shumë forma të ndryshme, duke përfshirë kompjuterët desktop, laptopët, kompjuterët kullë, sistemet e montuara në raft, minikompjuterët dhe kompjuterët mainframe. Pajisjet e tjera zakonisht lidhen me këto sisteme, duke përfshirë printerët, skanerët, ruterat, hard disqet e jashtme dhe pajisje të tjera ruajtëse, si dhe mbajnë prova elektronike.

Burimet elektronike të provave që duhet të kemi parasysh për kërkimin e provave elektronike janë:

1. Pajisjet e ruajtjes paraqiten në shumë forma dhe madhësi dhe ndryshojnë nga mënyra në të cilën ato ruajnë dhe mbajnë të dhëna. Ato mund të jenë:
   - Hard disqe dhe disqe solide
   - Media të lëvizshme
   - Karta memorieje
   - Pajisje USB të ruajtjes së të dhënave
   - Disqe me shirit për ruajtjen e të dhënave
   - Pajisje periferike

2. Pajisjet tableta
3. Telefonat celularë
4. Regjistrimet me foto dhe video
5. Provat Elektronike të mbajtura nga operatorët kombëtarë dhe ndërkombëtarë të shërbimeve të internetit

Llojet e provave elektronike nga kompjuterët dhe pajisjet e ruajtjes (Kriminalistika Digjitale)

Kategoritë e gjurmëve digjitale: Ashtu siç një kriminel lë pas gjurmë fizike në një skenë krimi, krimineli që kryen një krim me kompjuter do të lërë gjurmë në një "skenë krimi digjitale". Për të përftuar një ide më të mirë të tipeve të gjurmëve digjitale që mund të zbulojë një ekzaminues gjatë analizës kriminalistike, ka kuptim të bëhet dallimi midis dy tipeve të gjurmëve digjitale:

Gjurmët e shmangshme: Këto janë gjurmë që ruhen me parazgjedhje nga sistemi i shfrytëzimit dhe aplikacionet, por të cilat një sistem mund të konfigurohet të mos i ruajë. Merrni si shembull një shfletues në internet. Ky program do të ruajë historinë e shfletimit të një të dyshuari, si dhe detajet e shkarkimeve të tij ose të saj, plotësimet në formularë, cookies etj., por këto mund të çaktivizohen ose të fshihen nga i dyshuari.

Gjurmët e pashmangshme: Në të kundërt, gjurmët e pashmangshme janë, natyrisht, ato që nuk mund të çaktivizohen ose ato që kërkojnë përpjekje të konsiderueshme për t'u ndalur përkohësisht. Probabiliteti për të gjetur gjurmë të tilla është përkatësisht i lartë edhe nëse një i dyshuar është përpjekur të mbulojë gjurmët e tij/saj.

Çdo rast përfshin zakonisht disa gjurmë veçanërisht të rëndësishme. Në një rast mashtrimi, për shembull, dokumentet, tabelat dhe emailet janë zakonisht më të rëndësishme, ndërsa në rastet e abuzimit të fëmijëve fotografitë, videot dhe gjurmët e komunikimit janë më të rëndësishme. Por, edhe brenda atyre kategorive të rasteve, jo çdo rast është i njëjtë. Kjo është arsyeja pse nënkapitujt e mëposhtëm përfshijnë informacion mbi procedurat e mbështetura në llojin e tipit që ka lidhje dhe jo në tipin e rastit.

E-mailet: Për të analizuar komunikimin me e-mail, nuk është e rëndësishme vetëm të analizohen klientët e postës si Outlook, Thunderbird ose Mail, por edhe llogaritë e postës elektronike. Për të analizuar një klient të postës elektronike, është e

rëndësishme të dini se cilin artefakt prodhon ai klient. Për shembull, Outlook i ruan të dhënat e provave në skedarët e dosjeve personale, si skedarët PST, OST dhe PAB, ndërsa Thunderbird i ruan mesazhet në skedarë mbox. Kompletet e programeve kriminalistike zakonisht mund t'i analizojnë ata skedarë. Megjithatë, ata nuk i nxjerrin medoemos të gjitha mesazhet. Disa mjete kriminalistike, për shembull, kanë probleme në nxjerrjen e mesazheve të fshira nga skedarët e dosjeve personale.

Dokumentet e zyrës: Në rastet kur dokumentet e zyrës janë të rëndësishme, analisti i kriminalistikës digjitale duhet të kryejë një analizë të nënshkrimeve dalluese dhe më pas të filtrojë për skedarët me interes (p.sh. skedarët me nënshkrim docx). Kur analisti kriminalistik i ka gjetur ata skedarë, është praktikë e mirë, në varësi të politikave të zyrës, që ai t'i nxjerrë të gjithë ata skedarë dhe t'ia dorëzojë hetuesit të ngarkuar me çështjen për një analizë të përmbajtjes. Kur oficeri i çështjes ka identifikuar dokumentet përkatëse, analisti kriminalistik mund të kërkojë prova të mëtejshme se kur janë prodhuar ato dokumente, nga cili përdorues janë prodhuar dhe nëse janë dërguar apo pranuar nga persona të tjerë.

Foto/video: Shumica e zgjidhjeve softuerike të kriminalistikës ofrojnë mbështetje për analizimin në masë të fotografive dhe videove. Pas një analize fillestare të nënshkrimit të skedarit dhe vendosjes së një filtri për fotografitë dhe skedarët video, analisti i kriminalistikës mund të përdorë një pamje galerie për të inspektuar miniaturat e të gjitha fotografive për provat përkatëse të çështjes. Për një analizë më të shpejtë të skedarëve video, një program i caktuar ofron veçorinë e nxjerrjes së fotove të palëvizshme nga videot (p.sh. çdo X sekonda/minuta në varësi të cilësimeve). Këto imazhe të nxjerra më pas mund të shihen edhe në një pamje galerie.

Shfletuesit e internetit: Shfletuesit e internetit kanë një vlerë provuese për shumë raste. Zakonisht ato përmbajnë artefaktet e mëposhtme që duhet të analizohen: Historia e vizitave në faqe, memoria lokale / skedarët e përkohshëm të Internetit, faqeshënuesit / të preferuarat, informacionet e sesioneve, cookies, emrat e përdoruesve dhe fjalëkalimet e ruajtura, plotësimet e fushave të formularëve, kërkimet në Internet. Analizimi i artefakteve të shfletuesit mund të jetë i rëndësishëm për sugjerimin e qëllimit ose synimit (p.sh. fjalë kyçe të përdorura në motorët e kërkimit mund të provojnë synimin). Kjo është arsyeja pse ato artefakte duhet, në shumicën e çështjeve, të analizohen.

Artefaktet e softuerit: Çdo herë që një softuer i caktuar mund t'u shtojë vlerë provave çështjes, artefaktet e atyre programeve duhet të analizohen. Shembuj të programeve të tilla përfshijnë programet e komunikimit (p.sh. Viber, WhatsApp...), programet për shpërndarjen e skedarëve (p.sh. µTorrent), programet për kriptomonedha (p.sh. portofolet për Bitcoin), etj.

Aktiviteti i përdoruesit: Sistemi i shfrytëzimit i një kompjuteri gjurmon veprimtarinë e përdoruesit në shumë vende të ndryshme. Shembuj për këtë përfshijnë: kohën e ndezjes dhe mbylljes, cilësimet e programeve, listat e skedarëve të përdorur më së fundi, përdorimin e pajisjes, hyrjet e përdoruesve, lidhjet Wi-Fi, programet e preferuara, konfigurimin e mjedisit të përdoruesit dhe shumë të tjera. Analizimi i veprimtarisë së përdoruesit ndihmon për të kuptuar më mirë sjelljen e përdoruesit dhe madje mund të vërtetojë veprimtari provuese. Ato artefakte ruhen në vende të ndryshme, në varësi të sistemit të shfrytëzimit që është përdorur në kompjuter. Në Microsoft Windows, Registry, regjistrat e ngjarjeve dhe disa skedarë të tjerë duhet të analizohen nga ekzaminuesi. Në sistemet OS X, analisti do t'i gjejë shumicën e provave në dosjet e Bibliotekës dhe të regjistrave, ndërsa në sistemet Linux, shumica e të dhënave ruhen në dosjen kryesore të përdoruesit, në direktoritë "/etc" dhe "/var".

Skedarët e regjistrimit: Analizimi i skedarëve të regjistrimit është thelbësor veçanërisht në rastet e sulmeve kundër sistemeve. Analisti i kriminalistikës digjitale duhet të nxjerrë jo vetëm skedarët e alokuar të regjistrimit, por edhe gjurmët e skedarëve të fshirë/të paalokuar të regjistrimit. Për analizën e skedarëve të regjistrimeve disponohen programe të posaçme. Baza e një analize të tillë është ose kërkimi për fjalë kyçe të veçanta, kërkimi për modele jonormale ose kërkimi i regjistrimeve që kanë ndodhur brenda një afati kohor të caktuar.

Zonat e paalokuara: Zonat e paalokuara mund të përmbajnë artefakte të të gjitha llojeve të provave të përmendura më sipër. Kërkimi dhe nxjerrja e tipeve të caktuar të skedarëve në zona të paalokuara mund të automatizohet nga programi i gërmimit. Analistët e kriminalistikës digjitale duhet të përcaktojnë saktësisht se çfarë tipesh skedarësh po kërkojnë, pasi gërmimi për të dhëna është detyrë që kërkon shumë kohë. Gërmimi për të dhëna nuk funksionon mirë në skedarët e fragmentuar. Në shumicën e rasteve, të dhënat e gjetura në zona të paalokuara nuk mund të lidhen me një përdorues të caktuar apo madje me një vendndodhje brenda një strukture dosjeje.

Ruajtja në cloud/larg: Në situatat kur analistët e kriminalistikës gjejnë gjurmë të shërbimeve cloud që përdoren në një sistem kompjuterik, kjo mund të nënkuptojë që të dhënat e provave mund të ruhen jo vetëm në atë makinë, por edhe në largësi. Në fakt, të dhënat që ruhen larg mund të mos ruhen vetëm në një kompjuter të vetëm fizik, por në shumë serverë në "renë" kompjuterike. Në shumicën e rasteve, edhe ofruesi i një shërbimi cloud nuk mund të tregojë se në cilin server të caktuar, në cilën qendër të dhënash dhe në cilin vend ruhen pjesë të caktuara të të dhënave.

Kujtesa e kompjuterit (RAM): Kur përmbajtja e kujtesës së kompjuterit është përftuar ndërsa kompjuteri i sekuestruar ishte ende në punë, shkarkimi nga kujtesa mund të analizohet në laboratorin e kriminalistikës. Të kuptuarit e strukturave

të kujtesës në sisteme të ndryshme shfrytëzimi për të analizuar RAM-in është një detyrë shumë teknike. Kjo është arsyeja pse ajo duhet të bëhet vetëm nga ekzaminuesit që janë të kualifikuar për këtë punë. Për të analizuar shkarkimet e RAM-it nevojitet program i posaçëm. Artefaktet tipike që mund të nxirren nga shkarkimet e RAM-it përfshijnë: proceset në ekzekutim e sipër, përfshirë edhe kujtesën e tyre, informacionin e procesit (p.sh. dorezat), çelësat e kriptimit, skedarët e hapur, emrat e përdoruesve, fjalëkalimet, dokumentet e paruajtura.

Llojet e provave elektronike nga telefonat celularë (Kriminalistika digjitale)

Pajisjet celulare përmbajnë të dhëna dhe regjistrime të komunikimeve, së bashku me oraret dhe datat e komunikimeve në fjalë. Përveç kësaj, pajisjet celulare përmbajnë gjithashtu skedarë mediash dhe të dhëna vendndodhjeje që mund të përdoren gjatë një hetimi.

Kontaktet: Listat e kontakteve përbëjnë shtyllën mbështetëse të përdorimit të telefonit celular. Duhet pasur kujdes për të kryqëzuar artefakte të tjera të të dhënave me listat e kontakteve për të ndihmuar në identifikimin e subjekteve për hetim. Kontaktet mund të përfshijnë kanale të tjera komunikimi, informacion identiteti si dhe fotografi për të ndihmuar në identifikimin e individëve. Kontaktet mund të ndihmojnë gjithashtu në identifikimin e lidhjeve ndërmjet subjekteve dhe mundësisht të identifikojnë se për sa kohë ka ekzistuar një lidhje e tillë që nga datat e krijimit të kontakteve.

Regjistrimet e thirrjeve: Regjistrimet e thirrjeve shpesh përmbajnë vula date/kohe të krijuara nga ora e brendshme e celularit. Kjo mund t'i bëjë të pasigurta vulat e rikuperuara të orës/datës për të dhënat e thirrjeve. Shpesh, praktika më e mirë është mbledhja e informacionit të faturimit nga një operator i shërbimit celular për të konfirmuar informacionin e orës dhe datës për regjistrimet e thirrjeve. Kjo vulë kohore merret nga serverët e operatorit të shërbimit celular dhe kështu mund të konsiderohet e saktë (ose më mirë ka më shumë gjasa të jetë e saktë).

Artifaktet e aplikacioneve: Për shkak të sasisë së aplikacioneve të ndryshme dhe morisë së versioneve të aplikacioneve që janë të disponueshme, shpesh është e nevojshme të analizohen artefakte të ndryshme unike për aplikacione të ndryshme. Shumë prej këtyre aplikacioneve, për shembull, i ruajnë cilësimet në skedarët e bazave të të dhënave. Mund të ndodhë që skedarët e fshirë të bazave të të dhënave të rikuperohen dhe këto të mund të përdoren për të përcaktuar cilësimet e një aplikacioni në një pikë të caktuar në të kaluarën. Për shkak të natyrës së mbyllur të shumë aplikacioneve dhe mungesës së informacionit të disponueshëm,

shpesh mund të jetë e nevojshme të merret një pajisje testimi dhe të kryhen disa kërkime të drejtpërdrejta për të identifikuar vetitë e disa objekteve të aplikacionit.

Mesazhet me postë elektronike: Ashtu si me ekzaminimet e pajisjeve kompjuterike, komunikimet me postë elektronike në pajisjet celulare mund të përdoren brenda aplikacioneve të paracaktuara të postës elektronike dhe përmes postës në Internet të aksesuar përmes shfletuesit të internetit. Në disa pajisje, si p.sh. iPhone-ët më të rinj të Apple, nuk ofrohet mbështetje për nxjerrjen e mesazheve të postës elektronike nga aplikacioni i parazgjedhur i postës. Në këto raste ekzaminuesit do t'i duhet t'i regjistrojë të dhënat me dorë ose të përpiqet t'i mbledhë këto të dhëna nga burime të tjera.

Historiku i uebit: Shfletuesit e internetit në pajisjet celulare zakonisht ruajnë informacionin e mëposhtëm që mund të ketë vlerë provuese: artikujt e historisë së uebit, numërimi i vizitave të faqeve në ueb, faqeshënuesit / të preferuarat, cookies.

Provat elektronike që mbahen nga operatorët ndërkombëtarë të shërbimeve të Internetit (Kërkesa për Ruajtjen e të Dhënave, Kërkesa për Zbulimin e të Dhënave, MLA)

Të dhënat e pajtimtarëve:

Termi "informacion abonenti" nënkupton çdo informacion që ka mundësi të çojë në identifikimin e disa kategorive të informacionit që lidhen me pajtimtarin (pra përdoruesin) e komunikimeve elektronike. Kategori të tilla mund të përfshijnë tipin dhe të dhënat teknike të shërbimit të komunikimit të përdorur (përfshirë kohën), identitetin e pajtimtarit, adresën dhe të dhënat e kontaktit, si dhe çdo informacion tjetër në vendin e instalimit të pajisjeve të komunikimit. Këto informacione janë në formën e të dhënave kompjuterike ose çdo formë tjetër të mbajtur nga një operator shërbimi në lidhje me pajtimtarët e shërbimeve të tij (përveç të dhënave të përmbajtjes dhe të dhënave të trafikut). Ato të dhëna janë:

- Informacionet që kërkohen më shpesh në hetimet penale
- Më pak të ndjeshme ndaj privatësisë se sa të dhënat e trafikut dhe të dhënat e përmbajtjes
- Zakonisht mbahen nga operatorët e shërbimeve në sektorin privat, të përftuara nëpërmjet porosive të prodhimit

Të dhënat e trafikut: Termi "të dhëna trafiku" nënkupton çdo të dhënë kompjuterike që lidhet me një komunikim të realizuar me anë të një sistemi kompjuterik, të

krijuar nga një sistem kompjuterik që përbën një pjesë në zinxhirin e komunikimit, duke treguar origjinën e komunikimit, destinacionin, rrugën, kohën, datën, madhësinë, kohëzgjatjen ose tipin e shërbimit bazë.

Të dhënat e përmbajtjes: "Të dhënat e përmbajtjes" i referohen përmbajtjes së komunikimit; pra, kuptimi ose qëllimi i komunikimit, ose mesazhi apo informacioni që përçohet nga komunikimi (ndryshe nga të dhënat e trafikut). Ato të dhëna janë:

- Përmbajtja e komunikimit, pra kuptimi apo qëllimi i komunikimit, ose mesazhi apo informacioni që përcillet nga komunikimi (ndryshe nga të dhënat e trafikut)
- Përfshijnë përmbajtje të ruajtur dhe përmbajtje të ardhshme
- Për shembull, email-e, skedarë imazhesh, filmash, muzike e të tjera

Lloji i të dhënave të mbajtura nga operatorët ndërkombëtarë:

- Informacioni bazë i pajtimtarit (emri, adresa fizike, adresa e emailit dhe numri i telefonit) në lidhje me një llogari, si dhe regjistrimet e lidhjeve që mbahen deri në 30 ditë
- Regjistrimi themelor ose informacioni i klientit (emri, adresa, adresa e emailit dhe numri i telefonit) në lidhje me regjistrimin
- Informacioni i pajtimtarëve dhe regjistrimet e lidhjeve me adresat IP
- Informacioni i pajtimtarit (përfshirë detajet e kartës së pagesës) për transaksionet në dyqanet me pakicë të operatorëve të shërbimeve ose blerjet në internet
- Regjistrimet e lidhjeve
- Adresat MAC të pajisjeve
- Adresat IP dhe identifikuesit e tjerë të pajisjes që lidhen me aktivizimin e pajisjes nga sistemi i shfrytëzimit
- Informacioni i regjistrimit të pajtimtarëve dhe adresat IP të hyrjes dhe vulat kohore të lidhura për llogaritë;
- Informacioni i regjistrimit të pajtimtarëve, adresat IP të hyrjes dhe vulat kohore të lidhura, të dhënat e lidhjeve telefonike dhe informacioni i faturimit për llogaritë;
- Faqja e regjistrimit të blogut dhe informacioni i pajtimtarit të pronarit të blogut për Blogger
- Disa regjistrime ose informacione të tjera që kanë të bëjnë me llogarinë, pa përfshirë përmbajtjen e komunikimeve, të cilat mund të përfshijnë titujt e

mesazheve dhe adresat IP, përveç regjistrimit themelor të pajtimtarit

- Përmbajtja e ruajtur e çdo llogarie, e cila mund të përfshijë mesazhe, foto, video, postime në murin virtual dhe informacione për vendndodhjen.
- Të dhëna të tjera (në varësi të operatorit të shërbimit të internetit)

Më shumë informacion mund të gjendet në faqen e operatorit të shërbimit të internetit me informacione rreth bashkëpunimit me agjencitë e zbatimit të ligjit

Mbajtja/ruajtja e të dhënave

Mbajtja e të Dhënave: - Një kërkesë e përgjithshme për të ruajtur tipe të caktuara të dhënash komunikimi për një periudhë të caktuar kohore (zakonisht jo më shumë se 12 muaj)

Ruajtja e të Dhënave: – Ruajtja e të dhënave është një masë e cila lejon ruajtjen e përmbajtjes dhe të dhënave të tjera të trafikut të cilat nuk ruhen përmes mbajtjes së të dhënave.

Kriminalistika digjitale

Kriminalistika digjitale është degë e shkencës së kriminalistikës që fokusohet në identifikimin, marrjen, përpunimin, analizimin dhe raportimin e të dhënave të ruajtura në mënyrë elektronike. Provat elektronike janë përbërës të pothuajse të gjitha veprimtarive kriminale dhe mbështetja nga kriminalistika digjitale është thelbësore për hetimin e krimit.

Qëllimi kryesor i kriminalistikës digjitale është nxjerrja e të dhënave nga provat elektronike, përpunimi i tyre për të zbuluar informacion, mbi bazën e së cilit mund të ndërmerren veprime dhe paraqitja e provave në procesin e procedimit penal. Të gjitha proceset përdorin teknika të shëndosha kriminalistike për t'u siguruar që provat të jenë të pranueshme në gjykatë.

Kriminalistika e të Dhënave në Kohë Reale merret me situatat kur është e nevojshme që të dhënat të merren nga pajisjet përpara se ato të fiken apo të shkëputen nga rrjetet ose furnizimi me energji elektrike. Kjo lloj kriminalistike kërkon një nivel më të lartë specializimi sesa procedura e kërkimit dhe sekuestrimit të pajisjeve të fikura.

Në vitet e para të kriminalistikës digjitale ekzistonte rregulli i "heqjes nga priza" (*pull the plug*) sa herë që një hetues konstatonte një sistem funksional gjatë një procesi kërkimi dhe sekuestrimi. Në kohën e kaq shumë të dhënave të ndryshueshme në

kujtesë, lidhjeve në distancë dhe përdorimit të kriptimit, ky rregull doli jashtë loje. Shtënia në dorë dhe analizimi i të dhënave të tilla të ndryshueshme janë të një rëndësie të madhe, pasi mund të jenë me vlerë të lartë si prova. Kjo është një nga arsyet pse Kriminalistika e të Dhënave në Kohë Reale luan një rol të rëndësishëm në situatat e kërkimit dhe sekuestrimit në ditët e sotme.

Ekzaminimi kriminalistik i një sistemi të ndezur kërkon trajnim të posaçëm, përvojë praktike të drejtpërdrejtë dhe një grup mjetesh kriminalistike të pranuara si mjete të vlefshme. Nëse në vendngjarje nuk ndodhet një ekzaminues me këto aftësi, duhet të kërkohet menjëherë mbështetje nga njësia e posaçme. Nëse nuk gjendet askush, atëherë heqja e pajisjes nga priza mund të ketë më shumë kuptim sesa futja e duarve në prova, duke çuar në një kontaminim të mundshëm të tyre dhe duke e bërë të pamundur përdorimin në gjykatë.

Kriminalistika e të Dhënave në Kohë Reale merret me situatat kur është e nevojshme të merren të dhëna të ndryshueshme nga pajisjet përpara se ato të fiken ose të shkëputen nga rrjetet ose furnizimi me energji elektrike.

Të dhënat e ndryshueshme janë të dhënat që ruhen në mënyrë digjitale në mënyrë të tillë që ka një probabilitet shumë të lartë që përmbajtja e tyre të fshihet, të mbishkruhet ose të ndryshohet në një kohë të shkurtër nga ndërveprimi njerëzor ose i automatizuar. (Kujtesat *cache*, dokumentet që nuk janë ruajtur, proceset në ekzekutim e sipër, fjalëkalimet dhe çelësat e kriptimit, lidhjet e hapura në rrjet, informacionet e sistemit, përdoruesit që kanë hyrë në sistem, hapësira ruajtëse në largësi e lidhur përkohësisht, programet keqdashëse që ruhen vetëm në RAM)

Parimet e provave elektronike

Duhet të merren parasysh parimet e mëposhtme gjatë identifikimit dhe mbledhjes së provave elektronike. Jo të gjitha të dhënat në formë elektronike mund të pranohen si prova elektronike.

Integriteti i të dhënave: Asnjë veprim i ndërmarrë nuk duhet të ndryshojë materialisht asnjë të dhënë, pajisje elektronike apo mjet që mund të përdoret më pas si provë në gjykatë.

Pajisjet dhe të dhënat elektronike nuk duhet të ndryshohen, qoftë në lidhje me pajisjen apo programet. Personi i caktuar si personi përgjegjës për vendin e krimit ose për mbledhjen e provave është përgjegjës për ruajtjen e integritetit të materialit të gjetur dhe për sigurimin e zinxhirit kriminalistik të ruajtjes së të dhënave. Këtë përgjegjësi duhet ta marrin më pas persona të tjerë që duhet të caktohen si përgjegjës për pajisjet dhe/ose të dhënat. Kur të dhënat aksesohen në një pajisje të ndezur, kjo duhet të bëhet në atë mënyrë që të shkaktojë ndikimin

më të vogël tek të dhënat dhe nga një person i kualifikuar për ta bërë këtë.

Gjurma e auditimit: Duhet të regjistrohen dhe të ruhen të gjitha veprimet e ndërmarra gjatë trajtimit të provave elektronike, në mënyrë që më vonë ato të mund të auditohen. Një palë e tretë e pavarur jo vetëm që duhet të jetë në gjendje t'i përsërisë ato veprime, por edhe të arrijë të njëjtin rezultat.

Është e domosdoshme të regjistrohen me saktësi të gjitha veprimtaritë në vendngjarje për t'i mundësuar një pale të tretë të rindërtojë veprimet nëse është e nevojshme. E gjithë veprimtaria në lidhje me kërkimin, sekuestrimin, aksesin, ruajtjen ose transferimin e provave elektronike duhet të jetë plotësisht e dokumentuar, e ruajtur dhe e disponueshme për shqyrtim.

Çdo veprim i mëvonshëm në lidhje me përpunimin dhe ekzaminimin e provave elektronike duhet gjithashtu të jetë i përshtatshëm për auditim në të njëjtën mënyrë.

Mbështetja e Specializuar: Nëse pritet që gjatë një operacioni të planifikuar të gjenden prova elektronike, personi përgjegjës për operacionin duhet të njoftojë në kohë specialistët/këshilltarët e jashtëm dhe të marrë masa që ata të jenë të pranishëm nëse është e mundur.

Për hetimet që përfshijnë kërkimin dhe sekuestrimin e provave elektronike është gjithmonë e dëshirueshme që të përfshihen specialistë të provave elektronike kudo që është e mundur. Të gjithë këta specialistë, qoftë nga brenda organizatës, qoftë si kontraktorë të jashtëm, duhet të kenë njohuritë e duhura dhe objektivisht të verifikueshme për t'u marrë me provat elektronike siç duhet.

Trajnimi dhe certifikimi i duhur: Çdo person që merret me provat elektronike duhet të ketë trajnimin e nevojshëm dhe të përshtatshëm.

Në rrethanat kur nuk ka asnjë specialist në dispozicion, reaguesi i parë që kërkon, sekuestron dhe/ose akseson të dhënat origjinale të mbajtura në një pajisje elektronike ose media digjitale të ruajtjes duhet të trajnohet për ta bërë këtë sipas procedurave të sanksionuara ligjërisht dhe duhet të jetë në gjendje të shpjegojë dhe të justifikojë rëndësinë dhe implikimet e veprimeve të tij/saj.

Ligjshmëria: Personi dhe agjencia përgjegjëse për çështjen janë përgjegjës për t'u siguruar që ligji, masat mbrojtëse të provave dhe parimet e përgjithshme kriminalistike dhe procedurale të ndiqen një për një.

Pranueshmëria dhe paraqitja e një prove elektronike

Provat kompjuterike janë të pranueshme nëse janë në përputhje me një sërë ligjesh dhe rregullash që sigurojnë se janë të pranueshme nga gjykata. Gjatë marrjes së provave duhet të ndiqen procedurat e duhura. Këto janë artikuluar në kapitujt e mëparshëm.

Provat elektronike kanë për të qenë të pranueshme (mund të ndryshojnë nga juridiksioni në juridiksion) nëse gjatë kontrollit dhe sekuestrimit ndjekin kriteret minimale:

- Provat duhet të vërtetojnë faktet në një mënyrë që nuk mund të kontestohet dhe të jetë përfaqësuese e gjendjes së saj origjinale.
- Analiza ose çdo opinion i bazuar në prova duhet të tregojë të gjithë historinë dhe të mos i përshtatet një perspektive më të favorshme ose më të dëshiruar.
- Nuk duhet të ketë asgjë në lidhje me mënyrën e mbledhjes dhe trajtimit të provave që më pas mund të hedhë dyshime mbi vërtetësinë ose autenticitetin e tyre.
- Provat duhet të jenë bindëse sa u përket fakteve që përfaqësojnë dhe kushdo që ka përgjegjësinë e zbulimit të fakteve në procesin gjyqësor duhet të jenë në gjendje të mbështetet tek ato si prova të vërteta.
- Metodat e përdorura për mbledhjen e provave duhet të jenë të drejta dhe proporcionale me interesat e drejtësisë

Provat elektronike nuk janë të ndryshme nga provat fizike, si për shembull një dokument i regjistruar në një fletë letër. Është e nevojshme të garantohet që provat të jenë autentike. Dallimi midis provave elektronike dhe provave fizike është zakonisht lehtësia me të cilën provat elektronike mund të ndryshohen dhe të tjetërsohen, qoftë me apo pa dashje.

Në rast se ka dyshime për të dhënat elektronike të paraqitura si pjesë të provave, i takon mbrojtjes të ngrejë kundërshtime për pranueshmërinë e tyre. Në momentin që ngrihet kjo si çështje, me të duhet të merre prokuroria.

Një aspekt tjetër i rëndësishëm i provave është se si janë marrë ato dhe nëse metodologjia me të cilën është vërtetuar dëshmia është e përshtatshme për t'u vlerësuar në mënyrë objektive dhe shkencore. Për shembull, nëse prokuroria mund të paraqesë një faturë telefonike që tregon se i pandehuri është lidhur me ISP-në e tij në një orë të caktuar të ditës, atëherë kjo zakonisht pranohet si provë. Në të kundërt, nëse prokuroria pretendon se 'I pandehuri i ka fshirë të gjithë skedarët në hard diskun e tij, e ka riformatuar dhe më pas e ka hedhur nga një dritare e

katit të 10-të, por se prokuroria ka mundur t'i rindërtojë skedarët duke shkuar në një firmë të rikthimit të të dhënave", atëherë mbrojtja mund të vërë në dyshim vlefshmërinë e kësaj metode të rikthimit të provave. I takon prokurorisë që të demonstrojë se metodat e përdorura për të marrë provat kanë qenë të vlefshme dhe të bindë gjykatën që provat duhet të pranohen.

Provat elektronike trajtohen në gjykatë në të njëjtën mënyrë si çdo formë tjetër prove. Prokuroria do të duhet të provojë se dokumenti është autentik dhe se përmbajtja e tij është e pranueshme. Të gjitha veprimet me provat elektronike duhet të jenë në përputhje me parimet e provave elektronike.

Paraqitja e provave elektronike në gjykatë është më efektive nëse është vizuale, duke përdorur demonstrime kompjuterike, video demonstrim, grafika kompjuterike, tabela dhe grafikë. Megjithatë, prokurorët duhet të jenë të vetëdijshëm për paragjykimet që mund të shkaktojë përdorimi i një teknologjie të tillë dhe të jenë të përgatitur t'i diskutojnë këto çështje me autoritetet nëse mbrojtja e kundërshton përdorimin e një teknologjie të tillë.

PAJISJET ELEKTRONIKE/DIGJITALE: SI LIDHEN ATO ME HETIMET PENALE?

Kur punon si në një zyrë me rrjet kabllor ashtu edhe me rrjet pa tel, të dyja këto mjedise kanë një tipar të përbashkët: nevojiten si programe rrjeti ashtu edhe pajisje fizike (kabllo, rutera etj.) për të përçuar të dhëna nga pajisja juaj elektronike digjitale (për shembull, kompjuteri apo celulari) te një pajisje tjetër; brenda banesës suaj kjo kryhet në një rrjet privat.

Një proces i ngjashëm ndodh kur dëshironi të komunikoni me një pajisje mijëra kilometra larg tuajës në botën e jashtme, por ky proces përfshin rutimin për te një sistem adresimi unik për rrjete publike për të komunikuar me pajisjen përkatëse.

Kjo mund të merret si ngjashmëri me një sistem telefonik zyre apo hoteli ku ju formoni numra të brendshëm me të cilët të komunikoni (rrjet privat); por gjithashtu mund të lidheni me numra të jashtëm jashtë kufijve të rrjetit të brendshëm, duke formuar një sërë numrash të posaçëm dhe të lidheni nëpërmjet rrjeteve të operatorit të shërbimeve telefonike (rrjet publik).

Një pajisje digjitale ka tre identifikues digjitalë që veprojnë pak a shumë si adresë postare, për ta bërë të njohur se nga vjen komunikimi dhe ku të kthehet ai:

- Përdoruesi që ka bërë kërkesën (**Emri i përdoruesit/pajisjes**),
- Pajisja që ka bërë kërkesën (**adresat MAC**),
- Në cilin rrjet ndodhet pajisja (**adresa IP** në rrjetin lokal – LAN), dhe
- Nëse komunikimi dërgohet jashtë, në cilin rrjet do të dërgohet ai (**adresa IP** në rrjetin publik – WAN apo Internet).

Emri i përdoruesit: Disa pajisje elektronike digjitale (për shembull kompjuterët desktop apo ata laptop) lejojnë përdorimin nga më shumë se një person. Me qëllim që hollësitë e përdoruesve dhe dokumentet e tyre të mbahen private, secili përdorues ka një llogari me emër përdoruesi dhe shpesh me fjalëkalim, e cila siguron hapësira për ruajtjen e dokumenteve që lidhen me atë person dhe i japin mundësi personit që të hyjë në rrjet dhe/apo në Internet përmes pajisjes elektronike/digjitale.

Relevanca: Hetimet digjitale që merren me përcaktimin e lidhjeve mes pajisjeve dhe përdoruesve.

Emri i pajisjes: Ky është një emër që i jepet pajisjes. Këtë emër e shihni dhe/apo e vendosni në një nga ekranet e para që ju shfaqen kur e instaloni apo konfiguroni pajisjen nga e para.

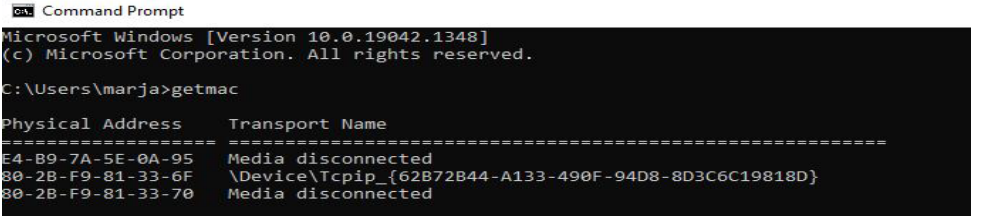
- Në përgjithësi, nëse pajisja është personale, personat i vendosin një emër që është personal për ta (për shembull, iPhone i Kastriotit apo Laptop-i i Anës);
- Në rastin e një kompanie, emri mund të fillojë me emrin e kompanisë (p.sh. BankaJonë-A345);
- Nëse pajisja ndodhet në rrjetin e një kompanie të madhe, ajo mund të referohet në mënyrë unike sipas një formati të paracaktuar (p.sh.: WIN-ABC-123).

Relevanca: Hetimet digjitale që merren me përcaktimin e lidhjeve mes pajisjeve dhe përdoruesve.

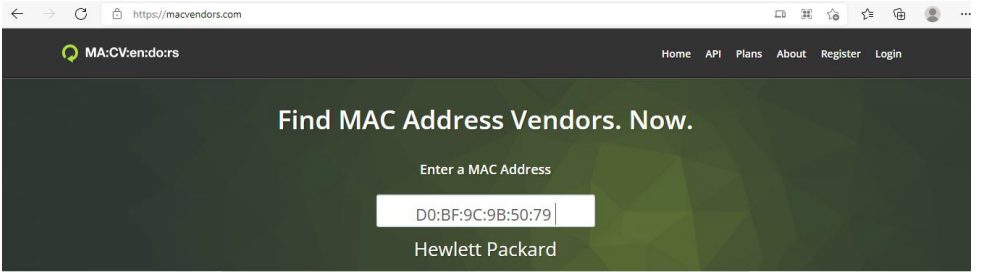
Adresat MAC: Për t'u lidhur në një rrjet apo me Internetin, pajisja ka nevojë për një kartë rrjeti (Network Interface Card - NIC). Secila kartë rrjeti ka një adresë fizike unike që njihet si Media Access Control (MAC).

Adresat MAC lidhen me pjesët fizike të kartave të rrjetit dhe shpesh referohen si adresa fizike rrjeti, apo adresa e shkruar (burned-in address - BIA), apo thjesht adresa fizike.

Ja një shembull adrese MAC për një kartë rrjeti: D0-BF-9C-9B-50-79. Një adresë MAC përbëhet nga 6 grupe me nga dy shifra apo shkronja, të ndara me viza apo dy pika. Adresa MAC address mund të gjendet përmes komandës "getmac" në *command prompt*.



Çdo karte rrjeti i jepet një adresë MAC gjatë prodhimit në fabrikë. Kjo adresë lidhet ngushtë me kartën e rrjetit (NIC) të kompjuterit tuaj dhe është numër unik. Për hetimet, adresa MAC është e rëndësishme për të identifikuar pajisjen në fjalë. Për më tepër, 6 karakteret (shkronjat dhe/ose numrat) e para identifikojnë prodhuesin e kartës. Ky informacion mund të gjendet falas në Internet në faqen www.macvendors.com. Me kryerjen e një kërkimi të tillë, tani unë e di që D0-BF-9C-9B-50-79 lidhet me një pajisje të prodhuar nga Hewlett Packard (HP), gjë që



mund të ndihmojë gjatë kërkimeve.

Një pajisje mund të ketë më shumë se sa një kartë rrjeti dhe, kështu, më shumë se sa një adresë MAC; pajisje të tilla janë:

- Kartat e rrjetave Ethernet (ky është xhepi ku futen kabllot gri apo të verdhë Cat5 që lidhin pajisjet me një prizë të ngjashme me ato të kabllove telefonike – rrjete të brendshme);
- Karta rrjeti për rrjete lokale pa tel (Wireless LAN) – (kjo është lidhja me Wi-Fi – më gjatë: 802.11 b/g/n Wi-Fi Adapter);
- Kartë për lidhje me Bluetooth – (kjo mundëson lidhjen e një pajisjeje Bluetooth në një rrjet personal);
- Kartë rrjeti virtuale për lidhje pa tel në një rrjet lokal – (Wi-Fi Direct Virtual Adapter), e cila i jep mundësi pajisjes që të bëhet pikë shpërndarëse (hotspot) Wi-Fi ose të përdoret për virtualizim. Nëse kjo është aktive, merrni në konsideratë nevojën për të kërkuar këshilla nga Njësia e Hetimit të Krimeve Kompjuterike.

Adresat MAC mund të manipulohen dhe të falsifikohen për qëllime kriminale apo për të fshehur identitetet; kjo njihet si “MAC spoofing”. Duke pasur parasysh këtë rast, jo gjithmonë mund të mbështetemi në relevancën e këtij informacioni.

Relevanca: Hetimet digjitale që merren me përcaktimin e lidhjeve mes pajisjeve dhe përdoruesve, me komunikimet dhe me rrjetat.

Rrjetet

Një rrjet kompjuterik është një grup kompjuterash të lidhur me njëri-tjetrin me qëllim që të ndajnë së bashku burime informacioni. Burimi që përdoret bashkërisht më së shpeshti në ditët e sotme është lidhja me Internetin. Burime të tjera mund të jenë një printer apo një server skedarësh.

NYJA është një pikë lidhjeje që mund të marrë, krijojë, ruajë apo dërgojë të dhëna përmes linjave të shpërndarjes në rrjete. Një pajisje kompjuterike e lidhur në rrjet

quhet gjithashtu NYJE. Një server është kompjuter që jep shërbime në rrjet dhe është NYJE.

LAN (Local Area Network) është rrjet lokal; kjo është zona përpara pajisjes lidhëse me Internetin, prandaj kjo përfshin rrjetin e brendshëm të një shtëpie, firme tregtare, shkolle etj.

WLAN është e njëjta gjë si LAN, por me lidhje pa tel (Wireless).

WAN (Wider Area Network) është një rrjet i madh si ai që mbulon një qytet të tërë, por më së shpeshti, në ditët e sotme, ky rrjet është Interneti.

Interneti është një rrjet masiv rrjetesh, një infrastrukturë rrjetesh. Ai lidh miliona kompjutera (NYJE) me njëri-tjetrin në të gjithë botën, duke formuar kështu një rrjet në të cilin çdo kompjuter mund të komunikojë me çdo kompjuter tjetër (NYJE) për sa kohë që të dy janë të lidhur në Internet.

Rrjetet **Peer-to-Peer** u lejojnë përdoruesve të lidhur në Internet që të krijojnë lidhje të drejtpërdrejta me kompjutera të tjerë rreth e përqark botës. Këto rrjete krijohen me qëllim shpërndarjen e skedarëve.

Relevanca: Hetimet digjitale në lidhje me komunikimet dhe rrjetat.

Serverat Një server është program kompjuterik që u ofron shërbime programeve të tjera kompjuterike (dhe përdoruesve të tyre) në të njëjtin kompjuter ose në kompjuterë të tjerë. Kompjuteri në të cilin funksionon një program server shpesh quhet gjithashtu server. Kjo makinë mund të jetë një server i dedikuar ose të përdoret edhe për qëllime të tjera. Emërtimet më të njohura të serverëve që mund të hasen janë:

Një server skedarësh është një kompjuter përgjegjës për ruajtjen dhe menaxhimin qendror të skedarëve të të dhënave në mënyrë që këto të mund të përdoren nga kompjuterë të tjerë në të njëjtin rrjet.

Një server proxy është program që vepron si ndërmjetës midis një pajisjeje fundore, siç është një kompjuter, dhe një serveri tjetër nga i cili një përdorues ose klient kërkon një shërbim.

Një server për e-mail (MX) është një aplikacion që merr e-mail nga përdoruesit lokalë (brenda të njëjtit domeni) apo nga dërgues të jashtëm dhe i përcjell këto email-e për dorëzim.

Serveri i Shërbimeve Emërore për Domenet (DNS) është ekuivalenti në Internet i një libri telefonik. Ai mban një listë të emrave të domeneve (www.asp.gov.al) dhe i përkthen ato në adresa numerike të Protokollit të Internetit (IP) (185.71.180.3). Pajisjet që lidhen me Internetin apo rrjete të tjera private mbështeten te serverat e

DNS për të gjetur adresat IP përkatëse të URL-ve (adresave të linqeve), të adresave të emailit dhe të emrave të tjerë të domeneve.

Kur kërkojmë një emër domeni, kompjuteri kërkon adresën IP që lidhet me emrin e kërkuar të domenit dhe krijon komunikim me adresën IP. DNS ka informacionin se cila IP i përgjigjet cilit emër domeni.

Një server Web-i është një program që përdor HTTP (Protokollin e Transferimit të Hipertekstit) për t'u shërbyer përdoruesve skedarët që formojnë faqe Web në përgjigje të kërkesave të tyre, kërkesa të cilat përcillen nga klientët HTTP të kompjuterëve të përdoruesve. Edhe kompjuterët dhe pajisjet e dedikuara mund të funksionojnë si, dhe të quhen gjithashtu, serverë web-i.

Relevanca: Hetimet digjitale në lidhje me përcaktimin e lidhjeve mes pajisjeve dhe përdoruesve, komunikimi dhe rrjeti, hetimi i emaileve, hetimi i faqeve të internetit, hetimi i shfrytëzimit të fëmijëve.

Adresa IP Adresa e protokollit të internetit (IP) është një etiketë numerike e caktuar për çdo pajisje (për shembull kompjuter, tabletë apo printer) që merr pjesë në një rrjet kompjuterik që përdor Protokollin e Internetit për komunikim. Disa adresa IP janë rezervuar dhe përdoren vetëm për një rrjet lokal privat (që lidh pajisjet tuaja në shtëpi ose zyrë) dhe disa adresa IP të tjera janë publike, për lidhje me rrjetet e jashtme (WAN/Internet). Adresat IP mund të jenë statike ose dinamike. Ekzistojnë 2 versione të adresave IP: IPv4 dhe IPv6.

Kush i përcakton adresat IP dhe nga vijnë të dhënat për to?

Autoriteti i Përcaktimit të Numrave në Internet (IANA) alokon dhe mirëmban kode unike dhe sisteme numerike unike që përdoren në standardet teknike ("protokollet") që drejtojnë internetin; këto mund të grupohen gjerësisht në tre kategori:

- Burimet e numrave - Koordinimi i grupit global të numrave të IP dhe të Sistemeve Autonome (AS), kryesisht duke ua ofruar ato Regjistrave

Rajonale të Internetit.

- Emrat e domeneve - Menaxhimi i rrënjës (bazës) së sistemit DNS, domeneve .int dhe .arpa dhe një burim të praktikave për IDN (*International domain name* - zgjidhje teknike për të përkthyer emrat e shkruar në alfabetet e gjuhëve jo latine, si: cirilike, kineze etj.).
- Përcaktimet e protokolleve - Sistemet e numërimit të protokolleve të Internetit menaxhohen bashkë me organizatat e standardeve.

Regjistri Rajonal i Internetit (RIR) është një organizatë që menaxhon shpërndarjen dhe regjistrimin e numrave të internetit duke përfshirë adresat IP dhe numrat e AS brenda një rajoni të caktuar të botës, për ofruesit e shërbimeve të internetit dhe organizatat e përdoruesve fundorë.

Janë 5 RIR:

- Qendra e Informacionit për Rrjetet Afrikane (AfriNIC) për Afrikën
- Regjistri Amerikan për Numrat e Internetit (ARIN) për Shtetet e Bashkuara, Kanadanë dhe disa pjesë të rajonit të Karaibeve
- Qendra e Informacionit për Rrjetet e Azisë dhe Paqësorit (APNIC) për Azinë, Australinë dhe vendet fqinje
- Qendra e Informacionit për Rrjetet e Amerikës Latine dhe Karaibeve (LACNIC) për Amerikën Latine dhe pjesë të rajonit të Karaibeve
- RIPE NCC për Evropën, Lindjen e Mesme dhe Azinë Qendrore

RIR-të shpërndajnë blloqe të adresave IP tek Operatorët e Shërbimeve të Internetit (ISP), të cilët nga ana e tyre u shpërndajnë klientëve adresa IP statike ose dinamike. Regjistri i blloqeve të adresave IP të alokuara duhet të mirëmbahet nga RIR.

Shtojca B tregon një shembull se çfarë informacioni do të ofrohet nga operatorët dhe mirëmbahet nga RIR.

Çfarë kemi nevojë të dimë për adresat IP?

Adresat IP Statike nuk ndryshojnë kurrë. Ato shërbejnë si adresë e përhershme në internet dhe ofrojnë një mënyrë të thjeshtë dhe të besueshme për kontaktimin nga kompjuterët në largësi. Adresat IP statike tregojnë informacione të tilla si kontinentin, shtetin, rajonin dhe qytetin në të cilin ndodhet një kompjuter, ISP-në (Operatorin e Shërbimeve të Internetit) që i shërben atij kompjuteri, si dhe informacione të tilla teknike si gjerësinë dhe gjatësinë e saktë gjeografike të vendit, si dhe kodin e gjuhës që përdor ai kompjuter.

Adresat IP Dinamike janë të përkohshme dhe vendosen çdo herë që një kompjuter hyn në Internet. Ato, në fakt, huazohen nga një grup adresash IP që ndahen mes

kompjuterëve të ndryshëm. Meqenëse numri i adresave IP statike të disponueshme është i kufizuar, shumë ISP rezervojnë një pjesë të adresave që u janë caktuar atyre për t'i ndarë mes abonentëve të tyre dhe përcaktojnë afate të kufizuara për lëshimin e tyre. Kjo ul kostot dhe u lejon atyre t'u shërbejnë më shumë abonentëve.

IPv4 – Versioni 4 i Protokollit të Internetit (Internet Protocol Version 4) është tipi më i njohur i adresave IP dhe përbëhet nga 4 grupe shifrash (çdo grup njihet si një oktet) që variojnë nga 0-255, për shembull 192.168.1.3 apo 77.28.81.50. Ashtu si me numrat e telefonit, disa blloqe numrash janë paracaktuar për t'u përdorur nga operatorët e shërbimeve, ndërsa disa të tjera janë ruajtur për arsye të tjera si kërkim-zhvillim. E njëjta gjë ndodh edhe me adresat IP.

Në një rrjet lokal (LAN), i cili është rrjet privat, blloqet e mëposhtme të adresave IP janë paracaktuar për t'u përdorur në konfigurimin e rrjeteve të brendshme:

- Klasa A: 10.0.0.0 – 10.255.255.255
- Klasa B: 172.16.0.0 – 172.31.255.255
- Klasa C: 192.168.0.0 – 192.168.255.255

Këto blloqe numrash nuk funksionojnë në rrjetet e jashtme, por vetëm brenda rrjeteve lokale si LAN dhe WLAN ku ruteri juaj do të ndajë automatikisht adresat IP private; në rrjete më të mëdha, ky proces konfigurohet nga administratori i rrjetit.

Secila pajisje e lidhur në rrjet ka nevojë për adresën e vet; kështu, për shembull, adresa 192.168.1.3 mund të identifikohet si një adresë private dhe në terma të thjeshtë ka të ngjarë të përdoret në një rrjet me adresa që variojnë nga 192.168.1.0 - 192.168.1.255.

Dy shembuj përjashtimesh nga ky rregull do të ishin:

- Kur një ruter lokal lejon lidhjen e vetëm 10 pajisjeve, atëherë adresat IP ka të ngjarë të jenë brenda një intervali prej 192.168.1.0 - 192.168.1.12.
- Në rrjetet e mëdha, administratorët e sistemit do të përdorin sa më shumë një numër të kufizuar adresash IP, duke përdorur një metodë të quajtur subnetting, që shpesh do të nënkuptojë se një adresë IP do të duket si kjo: 192.168.1.0/24. Kjo mënyrë mund të duket e ndërlikuar, por i jep mundësi rrjetit për të krijuar nënrrjete më të vogla dhe për të rritur numrin e përdorur të adresave IP, pak a shumë si një numër centrali telefonik që ka një numër shtesë për brenda një departamenti. - nëse hasni ndarje në nënrrjeta, kini parasysh që të kontaktoni CCIU për ndihmë të mëtejshme.

Adresat IP publike IPv4 janë adresa IP njëfundore të rutueshme globalisht dhe përdoren në një (WAN) dhe në Internet. Çdo adresë IP publike lëshohet nga një

Operator i Shërbimeve të Internetit dhe i përket brezit të numrave nga 1.0.0.0 në 191.255.255.255, me përjashtim të klasave të adresave private A dhe B:

(Klasa A: 10.0.0.0 – 10.255.255.255 / Klasa B: 172.16.0.0 – 172.31.255.255)

IPv6 Versioni 6 i Protokollit të Internetit (Internet Protocol Version 6) u prezantua pasi ishte parashikuar që, me rritjen e pajisjeve që kishin nevojë për t'u lidhur me WAN dhe Internet, sasia e disponueshme e adresave IPv4 do të mbaronte dhe për të parandaluar këtë u zhvillua IPv6.

Dallimi kryesor midis adresave IPv4 dhe IPv6 është gjatësia. Adresat IPv4 janë 32 bit dhe adresat IPv6 janë 128 bit. Për shkak të kësaj gjatësie masive, adresat IPv6 shkruhen duke përdorur një shënim tjetër nga adresat IPv4 dhe kjo i bën ato shumë të lehta për t'u dalluar nga adresat IPv4.

Numërimi me IPv6 kërkon 16 karaktere dhe përdor shifrat 0-9 dhe shkronjat e vogla a-f, të referuara si karaktere heksadecimale. IPv6 përbëhet nga 16 oktete, të paraqitura vizualisht si 8 segmente. Për shkak të gjatësisë masive të numrave, IPv6 përdor fshehjen dhe ngjeshjen e grupeve me zero për të thjeshtuar pamjen.

Kjo mund të tingëllojë komplekse, por do të thotë thjesht që IPv6 duket ndryshe dhe mund të shfaqet në ndonjë nga mënyrat e mëposhtme:

Kjo mund të duket si diçka komplekse, por thjesht nënkupton se IPv6 do të duket ndryshe dhe mund të shfaqet në cilëndo nga mënyrat e mëposhtme:

- 2001:0db8:0000:0000:0000:0000:0000:0001 (me 8 segmente/16 oktete – forma e plotë);
- 2001:db8:0:0:0:0:0:1 (fshehja e zerove lejon që 0-t fillestare të mos shfaqen);
- 2001:db8::1 (ngjeshja e zerove heq segmentet që përmbajnë 0 të njëpasnjëshme);
- Shënimi /64 në fund të secilit prej shembujve të mësipërm thjesht nënkupton nënrrjetin.

Pothuajse në çdo rast hetimor, IPv4 do të shfaqet dhe do të jetë fokusi kryesor i hetimit tuaj, por përherë e më shumë pajisje dhe serverë rrjeti po përfshijnë IPv6 në konfigurimin e tyre.

Adresat IP mund të manipulohen dhe falsifikohen për qëllime kriminale ose për të fshehur identitetet dhe kjo njihet si maskim (*spoofing*).

Relevanca: Të gjitha hetimet digjitale që merren me përcaktimin e lidhjeve mes pajisjeve dhe përdoruesve, me komunikimet, me rrjetat dhe me kërkesat për të dhëna komunikimi.

Protokollet

TCP/IP është protokolli mbi të cilin është ndërtuar Interneti; nuk është një protokoll i vetëm, por një grup i tërë protokollesh të ndërlidhura.

TCP (Protokolli i Kontrollit të Transmetimit) është një protokoll i orientuar drejt lidhjeve. TCP lejon komunikimet një me një duke i dhënë mundësi një pajisjeje të vetme rrjeti që të shkëmbejë të dhëna me një pajisje tjetër të vetme, në të njëjtin rrjet ose në një rrjet tjetër. TCP siguron që çdo paketë të dorëzohet nëse është e mundur. Këtë e bën duke vendosur një lidhje me pajisjen marrëse përpara dërgimit të paketave. Nëse një paketë nuk arrin, TCP e ridërgon paketën. Lidhja mbyllet vetëm pasi paketa të jetë dorëzuar me sukses ose të ketë ndodhur një gjendje gabimi e pandreqshme.

Shumë protokolle aplikacionesh mbështeten në TCP. Për shembull, kur një përdorues që po përdor një shfletues për web kërkon të hapë një faqe, shfletuesi përdor HTTP për të dërguar një kërkesë nëpërmjet TCP te serveri i web. Kur serveri i web merr kërkesën, ai përdor HTTP për t'ia dërguar faqen e kërkuar shfletuesit, përsëri përmes TCP. Protokollet e tjera të shtresës së aplikacioneve që përdorin TCP përfshijnë Telnet (për emulimin e terminalit), FTP (për shkëmbimin e skedarëve) dhe SMTP (për e-mail).

Relevanca: Të gjitha hetimet digjitale që merren me protokollet e komunikimit, rrjetat dhe manipulimet për sulme ndaj sigurisë kompjuterike.

ARP është një Protokoll i Zgjidhjes së Adresave për pajisje rrjeti; në përgjithësi, është ruteri ai që mban një tabelë kërkimi ARP ku ruhet informacioni se cilat adresa IP lidhen me cilat adresa MAC. Kjo mundëson që të dhënat të lidhen me dërguesin dhe marrësin e duhur. Tabelat janë një lloj logjike inteligjente: sa herë që merr një kërkesë, ruteri do të kontrollojë në tabelën e vet për të parë nëse rruga është e njohur, nëse jo, ai do të kërkojë në të gjithë rrjetin dhe, kur të identifikohet rruga, ai do të shtojë adresat MAC dhe IP në tabelë për referencë në të ardhmen. Tabelat ARP mund të manipulohen për qëllime kriminale dhe keqdashëse.

Relevanca: Të gjitha hetimet digjitale që merren me protokollet e komunikimit, rrjetat dhe manipulimet për sulme ndaj sigurisë kompjuterike.

World Wide Web (www.) përbëhet nga të gjitha burimet dhe përdoruesit në Internet që përdorin Protokollin e Transferimit të Hipertekstit (Hypertext Transfer Protocol - HTTP). Protokolli i hipertekstit tregohet në shfletues si http://www. dhe pasohet nga emri i domenit.

Protokolli i Transferimit të Hipertekstit

(Hypertext Transfer Protocol – HTTP) është një protokoll standard për faqet në web.

Hiperteksti është tekst që përmban "linqe" për te tekste të tjera; këtyre linqeve u referohemi zakonisht si hiperlinqe. Shpesh ato tregohen në dokumente nga nënvizimi me blu i tekstit dhe, kur klikohen, çojnë te një dokument apo faqe tjetër. Për shembull, nëse klikojmë te Policia e Shtetit shkojmë te http://www.asp.gov.al që njihet ndryshe si adresë në web.

Domeni është një grup kompjuterësh dhe pajisjesh në një rrjet që administrohen si një njësi me rregulla dhe procedura të përbashkëta. Brenda Internetit, domenet përcaktohen nga adresa IP. Të gjitha pajisjet që ndajnë së bashku një pjesë të adresës IP quhen se janë në të njëjtin domen.

Emrat e domeneve përdoren për të identifikuar një ose më shumë adresa IP. Për shembull, emri i domenit microsoft.com përfaqëson rreth një dyzinë adresash IP. Emrat e domeneve përdoren në URL për të identifikuar faqet e internetit.

Uniform Resource Locator (URL) dhe një adresë në web është e njëjta gjë në terminologjinë e Internetit dhe është adresa e plotë e faqes së internetit që po vizitojmë.

Një URL përbëhet nga këto pjesë: protokolli, emri i serverit, domeni i nivelit të lartë dhe shtegu i skedarit.

Si funksionon kjo? - Protokolli i tregon shfletuesit se si duhet të trajtohen të dhënat. Protokolli më i zakonshëm është HTTP; një tjetër është Protokolli i Transferimit të Skedarëve (FTP). Protokolli i një URL-je ndiqet gjithmonë nga dy pika dhe dy shenja fraksioni, p.sh., "http://" ose "mailto://".

Pas protokollit vjen emri i serverit, p.sh. "google.com." Kjo është direktoria e kreut të faqes të Google, nga e cila buron gjithçka në direktorinë e Google. Pjesa ".com" quhet domen i nivelit të lartë; ai përdoret për kompjuterët në Shtetet e Bashkuara dhe për të treguar llojin e entitetit që krijoi faqen e internetit.

Një **nëndomen** është domen që bën pjesë në një domen më të madh, për shembull: ".gov.al".

Shtegu i skedarit është pjesa e fundit e URL-së dhe tregon skedarin specifik në server që duhet të aksesohet. Për shembull: http://www.asp.gov.al/drejtori-i-pergjithshem-i-policise-se-shtetit/ kërkon faqen e profilit për Drejtorin.

http:// - Protokolli i Internetit

www.asp.gov.al – emri i domenit

Protokolli i Sigurtë i Transferimit të Hipertekstit (Hypertext Transfer Protocol Secure - HTTPS) është një protokoll për komunikim të sigurt përmes një rrjeti kompjuterik dhe përdoret gjerësisht në internet brenda një lidhjeje të kriptuar **nga** Sigurimi i Shtresës së Transportit. Motivimi kryesor për HTTPS është vërtetimi i faqes së internetit të vizituar, faqet e sigurta të pagesave dhe mbrojtja e privatësisë dhe integritetit të të dhënave të shkëmbyera.

Protokolli i Transferimit të Skedarëve (FTP) është një protokoll standard rrjeti që përdoret për të transferuar skedarë kompjuterikë midis një klienti dhe serveri në një rrjet kompjuterik (ftp:// etj). FTP është ndërtuar sipas arkitekturës së modelit klient-server dhe përdor lidhje të ndara për kontrollin dhe shkëmbimin e të dhënave midis klientit dhe serverit.

Përdoruesit e FTP mund ta vërtetojnë veten me një protokoll hyrjeje me tekst të hapur, zakonisht në formën e një emri përdoruesi dhe fjalëkalimi, por mund të lidhen në mënyrë anonime nëse serveri është konfiguruar për ta lejuar këtë. Për transmetim të sigurt që mbron emrin e përdoruesit dhe fjalëkalimin dhe shifron përmbajtjen, FTP shpesh sigurohet me SSL/TLS (FTPS), këto janë komunikimet e sigurta dhe të kriptuara.

Serverat FTP dhe FTPS ndeshen shpesh gjatë hetimeve për shkeljet e prodhimit dhe shpërndarjes së pornografisë për fëmijë, pasi këto protokolle përdoren nga kriminelët për të shkëmbyer materiale.

Mailto është një skemë Identifikuesi të Njëtrajtshëm të Burimeve (URI) për adresat e emailit. Përdoret për të prodhuar hiperlidhje në faqet e internetit që lejojnë përdoruesit të dërgojnë një email në një adresë specifike pa pasur nevojë më parë ta kopjojnë atë dhe ta futin atë në programin për email.

Në vijim tregohen shembuj të secilit prej gjashtë protokolleve:

Protokollet	Domeni	Nëndomeni i TLD	Domeni i nivelit të lartë (TLD)	Adresa IP
http://	asp	.gov	.al	185.71.180.28
http://	google		.com	8.8.8.8
https://	paypal		.com	2.20.33.150
ftp:// & ftps://	192.168.1.1			192.168.1.1
mailto://	emri@email		.com	

DOMENI zotërohet nga një entitet dhe sigurohet nga një regjistrues

- Domeni i WIKIPEDIA: wikipedia.org

SHËRBIMI sigurohet nga entiteti brenda domenit

- Faqja në web: www.wikipedia.org
- Shërbimi i e-mail: smtp.wikipedia.org
- Shkëmbimi i skedarëve: ftp.wikipedia.org

Regjistrimi i Domeneve

Kur regjistroni një emër domeni, Korporata e Internetit për Emrat dhe Numrat e Alokuar (ICANN) kërkon që regjistruesi i emrit të domenit tuaj të dorëzojë të dhënat tuaja të kontaktit në bazën e të dhënave WHOIS. Pasi listimi juaj të shfaqet në direktorinë WHOIS të domeneve në Internet, ai është i disponueshëm publikisht për këdo që zgjedh të kontrollojë emrat e domeneve duke përdorur mjetin e kërkimit WHOIS.

Ka përjashtime:

- Aty ku përdoren agjentët e palëve të treta (Kompanitë e Privatësisë) për të regjistruar domenin, të dhënat e vërteta të pronarit të domenit nuk do të jenë të pranishme (në ato raste do të kemi nevojë të përdorim mekanizma të bashkëpunimit ndërkombëtar).
- Aty ku është dhënë informacion i rremë (bashkëpunim ndërkombëtar, kërkesë MLA).

Mjete kërkimi dhe baza të dhënash online për analizimin e adresave IP dhe domeneve

Ekzistojnë një numër shërbimesh online, si falas ashtu dhe me pagesë, për ekzaminimin e adresave IP me nivele të ndryshme saktësie. Të gjithë i marrin të dhënat e tyre nga RIR, por disa e realizojnë këtë nëpërmjet një shkarkimi të vetëm ose shkarkimeve periodike, ndërsa të tjerët lidhen më shpesh me bazën e të dhënave të RIR. Një tregues është data e ndryshimit të fundit të regjistrimit; prandaj ia vlen të kontrolloni tuaj edhe te shërbime të tjera për të konfirmuar se keni informacionin më të freskët.

Shërbime falas – Tipet e kërkesave:

- Kërkim në Whois – Adresa IP dhe domene
- Kërkim në Whois për IP

- Kërkim domeni
- Kërkim i anasjelltë Whois
- Kërkim i anasjelltë për adresat IP
- Kërkim i anasjelltë për të dhënat e NS
- Kërkim i anasjelltë për të dhënat e MX
- Kërkim i anasjelltë në Whois për të dhënat e adresaveIP

Mjete për hetimin e adresave IP

- www.iptracking.com
- www.centralops.net
- www.ipaddress.com

Shumë të tjera

Shihni Shtojcën A – Si të kërkoni një adresë IP.

Shihni Shtojcën B – Shpjegimi i regjistrimeve të të dhënave në Regjistrat Rajonalë të Internetit.

Relevanca: Hetimet digjitale, Hetimet për sigurinë kompjuterike, Gjetja e atributeve të faqeve, dhe përftimi i të dhënave të telekomunikimit.

E-mail

Komunikimi me email trajtohet në shumë hetime penale dhe jo vetëm për krimet kompjuterike. Analizimi i kokave të mesazheve email mund të identifikojë dërguesit e emaileve kërcënuese, abuzive apo të identifikojë adresat e rreme të email në mesazhe të padëshiruara, të kamufluara apo mashtruese. Kontrollimi i kokës së emailit dhe adresës IP në listat e zeza shpesh mund të konfirmojë nëse mesazhi është pjesë e një vepre penale.

Email-i mund të mbështetet në web ose në program klient dhe përdor tre lloje të Protokollit të Postës. Këta faktorë, së bashku me vendin ku ruhet mesazhi, mund të duhet të merren parasysh gjatë një hetimi.

Email në Web – emaili përpilohet dhe shikohet në një faqe interneti përmes një klienti email-i të ndërtuar si një aplikacion për web dhe që funksionon në një server web-it, për shembull Gmail, AOL dhe Yahoo.

Email mbështetur në programe – është leximi i postës elektronike të dërguar dhe të marrë duke përdorur një program për email të instaluar në kompjuterin/ pajisjen tuaj, (për shembull Microsoft Outlook, Mozilla Thunderbird, apo Mail për përdoruesit e Apple).

Tre Protokollet për Email janë:

- Simple Mail Transfer Protocol (SMTP) për dërgimin e email
- Post Office Protocol version 3 (POP3) për marrjen e email-eve nga një server
- Internet Message Access Protocol (IMAP) për marrjen e email-eve nga një server

Analizimi i kokave të plota të email shpesh do të thotë që të dhënat lexohen nga kreu në fund për të përcaktuar:

Shfaqjet e para të:	Informacion tjetër që mund të ndihmojë me identifikimin e pajisjes së përdorur:
Informacionit për dërguesin	Përshkrimi i programit të email
Adresës IP origjinale, me kohën origjinale të mbërritjes	Gjuha e programit
Dërguesit të parë me adresë të jashtme për ISP-në	Informacion lokal për pajisjet
Dërguesit të parë me adresë të brendshme IP	Informacion lokal për email

Shënim: Çështjet e privatësisë të ngritura kohët e fundit kanë bërë që disa kompani t'i heqin këto të dhëna nga email-et ose t'i shifrojnë këto të dhëna, të cilat bëhen kështu të palexueshme në kokën e email.

Mjete online për analizimin e kokave të email-eve:

Më poshtë vijojnë shembuj të mjeteve falas në Internet që disponohen për analizimin e kokave të plota të email:

- www.iptrackeronline.com – Kërkim për adresa IP, Analizues për Email që tregon vendndodhjen gjeografike për adresën IP të dërguesit, Lokalizues për Regjistrimet e Domeneve, si dhe mjete të tjera.
- www.mxtoolbox.com – Analizues për Email, Kërkim për Serverin e Email, Lista të Zeza për Email për të ulur spam, Diagnostikues për SMTP dhe mjete të tjera.

Shtojca C – Hetimi i Email jep më shumë informacion për funksionimin e email, protokollet e rrjetit për komunikim, ku ruhen të dhënat, ku mund të gjeni të dhënat e kokës së emailit dhe cilat të dhëna të përfshira në kokat e emailit mund të ndihmojnë në hetimet penale.

Relevanca: Hetimi i Email, Hetimet Digjitale, Ruajtja dhe Përftimi i të Dhënave të Komunikimit, Traktati i Ndihmës Ligjore të Ndërsjelltë, Agjencitë Ndërkombëtare të Policisë dhe Gjykatave, Qasja në Bazat e të Dhënave të Shërbimeve Informative Ndërkombëtare.

Përftimi i të dhënave të komunikimit si prova

Të dhënat e komunikimit janë informacioni rreth një komunikimi. Ky informacion përfshin kohën dhe kohëzgjatjen e një komunikimi, numrin ose adresën e emailit të autorit dhe marrësit; mund të sigurojë vendndodhjen e pajisjes nga e cila është bërë komunikimi.

Të dhënat e komunikimit nuk përfshijnë përmbajtjen e ndonjë komunikimi, teksti të një emaili ose një bisede në telefon. Është informacion për komunikimin, jo vetë komunikimi.

Të dhënat e komunikimeve përdoren në hetimin e të gjitha llojeve të krimeve, përfshirë krimet kompjuterike dhe terrorizmin. Ato i mundësojnë policisë të krijojë një pamje të veprimeve, kontakteve dhe vendndodhjes së një personi që është nën hetim dhe mund të përdoren si provë në gjykatë.

Një Operator i Shërbimeve të Komunikimit (CSP) ose Operator i Shërbimeve të Internetit (ISP) detyrohet me ligj që të ruajë lloje të caktuara të të dhënave të komunikimit, aty ku ata kanë arsye pune për t'i gjeneruar ose përpunuar ato. Prokurori mund të aplikojë për të marrë akses në të dhënat e komunikimit - sipas Kodit të Procedurës Penale (KPP) të Republikës së Shqipërisë, që me raste ka të bëjë me masat e posaçme hetimore - nëse mund të tregojë se kërkesa e saj është e nevojshme dhe proporcionale. Qasja jepet rast pas rasti dhe policia nuk ka pushtet për të marrë akses në të dhënat e komunikimit kur ato nuk janë të lidhura me një hetim apo operacion konkret.

Një direktivë e BE-së për ruajtjen e të dhënave rekomandon që CSP-të dhe ISP-të të ruajnë disa të dhëna komunikimi të lidhura me telefoninë dhe Internetin, të dhëna të cilat gjenerohen ose përpunohen në lidhje me punën e tyre, për 6 deri në 24 muaj. Periudha e ruajtjes në Republikën e Shqipërisë është 12 muaj.

Çfarë lloj të dhënash komunikimi janë në dispozicion?

Tre kategori të dhënash janë në dispozicion: të dhënat e pajtimtarit, të dhënat e përdoruesit të shërbimit dhe të dhënat e trafikut.

Të dhënat e Pajtimtarit

Janë të dhëna që mbahen nga CSP-të e sektorit privat për njerëzit të cilëve u ofrojnë një shërbim (për shembull emrat, adresat, numrat e telefonit, emri i mbajtësit të llogarisë, mënyrat e pagesës, numrat fiskalë);

- 'Kontrollet e abonentëve' (të njohura edhe si 'kërkime të anasjellta') të tilla si "kush është abonenti i numrit të telefonit **00 355 69 1234567**?", "kush është mbajtësi i llogarisë së postës elektronike example@example.al?" ose "kush ka të drejtë të postojë në faqen **www.shembull.al** ?";
- Informacion lidhur me pajtimtarin e një numri Kutie Postare ose një Shënimi Parapagimi që përdoret në postimet me shumicë;
- Informacion në lidhje me ofrimin për një pajtimtar ose mbajtës të llogarive të shërbimeve të përcjelljes/ridrejtimit, përfshirë edhe adresat e dorëzimit dhe dërgimit;
- Informacioni për llogarinë e pajtimtarëve ose mbajtësve të llogarisë, përfshirë emrat dhe adresat për instalim, dhe faturimin duke përfshirë mënyrën/-at e pagesës, detajet e pagesave, numrat fiskalë;
- Informacion për lidhjen, shkëputjen dhe rilidhjen e shërbimeve të cilat janë rezervuar nga, apo në të cilat është abonuar (ose mund të jetë abonuar), pajtimtari ose mbajtësi i llogarisë, përfshirë thirrjet në grup, mesazhet e thirrjeve, shërbimet e telekomunikacionit të pritjes dhe ndalimit të thirrjeve, dhe adresat IP që mund të jenë statike;
- Informacion në lidhje me aparatet e përdorura ose të vëna në dispozicion të pajtimtarit ose mbajtësit të llogarisë, duke përfshirë prodhuesin, modelin, numrat serialë dhe kodet e aparatit;
- Informacioni që i ka dhënë një CSP-je një pajtimtar ose mbajtës llogarie, si informacion demografik ose të dhënat e pajtimit (në masën që informacioni, siç është një fjalëkalim, që jep akses në përmbajtjen e çdo komunikimi të ruajtur nuk zbulohet, përveçse kur kërkohet sepse një informacion i tillë është i nevojshëm në interes të sigurisë kombëtare).

Informacioni për Përdorimin e Shërbimit

është informacion në lidhje me përdorimin e një shërbimi nga një person. Shembujt përfshijnë:

- Të dhënat e detajuara të thirrjeve telefonike (numrat e thirrur);
- Të dhënat e detajuara të lidhjeve me shërbimet e Internetit;
- Koha dhe kohëzgjatja e detajuar e përdorimit të shërbimit (thirrjeve dhe/ose lidhjeve);
- Informacion për sasinë e të dhënave të shkarkuara dhe/ose të dërguara;
- Informacion në lidhje me përdorimin e shërbimeve të caktuara për përdoruesin, ose në të cilat është abonuar (ose mund të jetë abonuar) përdoruesi, përfshirë thirrjet në grup, mesazhet e thirrjeve, vendosja në pritje e thirrjeve dhe ndalimi i thirrjeve;
- Informacion rreth përdorimit të shërbimeve të përcjelljes/ridrejtimit;
- Informacione rreth zgjedhjes së numrave të preferuar ose thirrjeve me kosto të ulur;
- Regjistrimet e dërgesave postare, të tilla si regjistrimet e postës së regjistruar, dërgesave postare të regjistruara ose të posaçme, të dhënat e dërgesës, dorëzimit dhe grumbullimit të kolive.

Të dhënat e Trafikut

janë informacion rreth një komunikimi dhe pajisjeve të përdorura në transmetimin e tij, përfshirë edhe:

- informacion që gjurmon origjinën ose destinacionin e një komunikimi që është ose ka qenë në transmetim (përfshirë regjistrimet e thirrjeve hyrëse);
- informacion që identifikon vendndodhjen e aparatit kur po kryhet, është kryer ose mund të kryhet apo marrë një komunikim (si p.sh. vendndodhja e një telefoni celular);
- informacion që identifikon numrin ID të dërguesit ose marrësit (përfshirë marrësit e kopjeve) të një komunikimi nga të dhënat e përfshira ose të bashkangjitura në komunikim;
- informacion rutimi që identifikon aparaturën përmes të cilës po transmetohet ose është transmetuar një komunikim (për shembull, dhënia

e një adrese IP dinamike, regjistrimet e transferimit të skedarëve dhe kokat e postës elektronike - deri në masën që përmbajtja e një komunikimi, siç është titulli i një mesazhi e-mail, nuk zbulohet)

- Informacioni i shfletimit të internetit në masën që zbulohet vetëm një makinë mbartëse, server, emër domaini ose adresë IP;
- çdo gjë, të tilla si adresat ose shenjat, të shkruara në pjesën e jashtme të një artikulli postar (si letër, kuti ose koli) që është në transmetim dhe që tregon rrugëtimin postar të artikullit;
- regjistrimet e kontrolleve të korrespondencës që përmbajnë detaje të të dhënave të trafikut nga dërgesat postare gjatë transmetimit deri te një adresë specifike;
- Ndjekja online e komunikimeve (përfshirë dërgesat postare dhe pakot).

Kur mund të përftojmë të Dhëna Komunikimi

- Për interesa të sigurisë kombëtare;
  Prokurori mund të aplikojë për një urdhër nga Gjykata e Lartë.
- Me qëllim të parandalimit ose zbulimit të krimeve ose parandalimit të shkeljeve të rendit;
  Sipas KPP, masat e posaçme hetimore.
- Provat mund të përdoren vetëm për rastin për të cilin janë kërkuar ose urdhëruar.
  Të dhënat e komunikimit mund të merren për një kohë të kufizuar.

Procedurat për Mbledhjen e të Dhënave të Komunikimit – Operatori Kombëtar i Shërbimeve të Komunikimit:

Policia:

1. Identifikoni tipin e të dhënave të kërkuara.
2. Identifikoni krimin dhe nenin e ligjit me të cilin lidhet.
3. Merrni parasysh qëllimin e kërkesës për të dhëna - ‘a është e nevojshme dhe proporcionale’?
4. Me të dhënat IP kini parasysh adresat IP dinamike:

a. përcaktoni datën (nëse ofruesi ndodhet jashtë shtetit, emërtoni muajin për të shmangur ngatërresat pasi SHBA përdorin mm/dd/vvvv dhe Mbretëria e Bashkuar/Evropa përdorin dd/mm/vvvv),
b. koha (hh:mm:ss) e veprimit,
c. kini parasysh brezin orar në vulën kohore (përfshijini këto në çdo aplikacion së bashku me shpjegimin e llogaritjeve ose konvertimit në UTC ose PST)

5. Çdo parashtrim duhet të kryhet në prokurori.

Prokuroria:

Për të marrë informacionin për pajtimtarin mund të aplikohet te, dhe merret nga, prokuroria:

1. Prokuroria i dërgon urdhër operatorit të shërbimeve ose merr urdhër nga gjykata
2. Nëse prokuroria konstaton se provat kanë lidhje me çështjen dhe janë të një standardi të pranueshëm.
3. Prokuroria merr një urdhër gjykate.
4. Prokuroria i dërgon kërkesë zyrtare Operatorit të Shërbimeve.
5. Operatori i Shërbimeve i kthen përgjigje prokurorisë.

Për të marrë informacionin për shërbimet dhe të dhënat e trafikut mund të aplikohet te, dhe merret nga, prokuroria:

1. Hetuesi i dërgon kërkesë/propozim prokurorisë.
2. Nëse prokuroria konstaton se provat kanë lidhje me çështjen dhe janë të një standardi të pranueshëm.
3. Prokuroria i dërgon kërkesë zyrtare Operatorit të Shërbimeve.
4. Operatori i Shërbimeve i kthen përgjigje prokurorisë.
5. Prokuroria i kthen përgjigje hetuesit.

Shërbimi Postar:

1. Policia informon prokurorinë.
2. Prokuroria kërkon urdhër nga gjykata. Duhet të paraqiten prova reale, jo vetëm një dokument rreth provave.
3. Gjykata mund të thërrasë në gjyq një përfaqësues të shërbimit postar.
4. Nëse provat janë të mjaftueshme, gjykata jep urdhër sipas dispozitave të KPP.

Procedura për Marrjen e të Dhënave të Komunikimit (Jashtë Shqipërisë)

CSP/ISP-të ndërkombëtare nuk i nënshtrohen të njëjtave rregullore për ruajtjen e të dhënave të komunikimit ashtu si në Shqipëri ose Evropë, që do të thotë se të dhënat dhe provat e komunikimit mund të humbasin.

Kjo, së bashku me faktin se kërkesat ndërkombëtare shpesh duhet të mbështeten me një ***Kërkesë në kuadër të Traktatit për Ndihmë Ligjore Reciproke*** (MLAT) ose Letër-Porositë e Komisionit duhet të dorëzohen përmes kanaleve gjyqësore dhe diplomatike, shpesh nënkupton që të dhënat dhe provat mund të humbasin.

Për të zbutur këtë problem, mund të dërgohet nga Policia në Polici një ***Kërkesë për Ruajtjen e të Dhënave***, e cila zakonisht skadon pas 90 ditësh; përpara mbarimit të këtij afati duhet të dërgohet një kërkesë e mëtejshme 90-ditore nëse të dhënat nuk janë marrë, për të lënë kohë për paraqitjen e një kërkese në kuadër të MLAT.

Në përgjithësi, kërkesat për ruajtje dërgohen nëpërmjet Departamentit të Bashkëpunimit Policor Ndërkombëtar (DBPN), i cili përcakton se cili partner ndërkombëtar është kanali më efektiv për Kërkesën për Ruajtje të të Dhënave. Kjo nuk do të thotë se të dhënat do t'i tregohen policisë, ky është kanali për të lehtësuar procesin e dërgimit të kërkesës MLA.

Prokuroria:

Identifikoni tipin e të dhënave të kërkuara.

1. Identifikoni krimin dhe nenin e ligjit me të cilin lidhet.
2. Identifikoni emrin dhe informacionin e kontaktit të operatorit të shërbimeve të Internetit që mban të dhënat.

3. Identifikoni shtetin nga juridiksioni i të cilit mbulohet ofruesi i shërbimeve të Internetit.

4. Merrni parasysh qëllimin e kërkesës për të dhëna - 'a është e nevojshme dhe proporcionale'?

5. Dërgoni kërkesën për ruajtjen e të dhënave (Formulari për Kërkesën për Ruajtjen e të Dhënave, Shtojca 3)

6. Me të dhënat IP kini parasysh adresat IP dinamike:

   - përcaktoni datën (nëse operatori ndodhet jashtë shtetit, emërtoni muajin për të shmangur ngatërresat pasi SHBA përdorin mm/dd/vvvv dhe Mbretëria e Bashkuar/Evropa përdorin dd/mm/vvvv),
   - koha (hh:mm:ss) e veprimit,
   - kini parasysh brezin orar në vulën kohore (përfshijini këto në çdo aplikim së bashku me shpjegimin e llogaritjeve ose konvertimit në UTC ose PST)

7. Çdo parashtrim duhet të kryhet nga prokuroria, zakonisht kërkesa për ruajtjen e të dhënave i dërgohet DBPN-së.

8. Dërgoni kërkesën MLA (Formulari për Kërkesën për Ruajtjen e të Dhënave, Shtojca 2)

9. Shumica e kërkesave për ruajtje të dhënash zgjasin 90 ditë, mund të dërgohet kërkesë për shtyrjen e periudhës së ruajtjes, përpara se të mbarojë afati 90-ditor, për t'u siguruar që të dhënat të mos humbasin përpara se ato të merren zyrtarisht përmes një kërkese në kuadër të MLAT.

Relevanca: Hetimet mbi Email, Hetimet Digjitale, Ruajtja dhe marrja e të Dhënave të Komunikimit, Traktati për Ndihmën Ligjore Reciproke, Policia Ndërkombëtare dhe Agjencitë Gjyqësore.

Partnerët ndërkombëtarë dhe kombëtarë

Departamenti i Bashkëpunimit Policor Ndërkombëtar (DBPN) EPH - Europol - Eurojust - Interpol – SELEC

DBPN-ja e ka selinë në Tiranë dhe është përgjegjëse për koordinimin e Partneriteteve Ndërkombëtare për të luftuar krimin e organizuar ndërkombëtar. DBPN-ja përbëhet nga:

- Njësia e Byrosë Qendrore Kombëtare të Interpol-it – BQK Tiranë;
- Europol – duke përfshirë ndërlidhjen me zyrën e prokurorisë për operacionet me Eurojust-in;
- Qendra Juglindore e Zbatimit të Ligjit (South East Law Enforcement Centre) – SELEC Shqipëri;

DBPN-ja koordinon punën me partnerët, duke u fokusuar në fushat e mëposhtme të krimit:

- Trafiku i Drogës;
- Siguria Publike dhe Terrorizmi;
- Trafikimi i qenieve njerëzore;
- Emigracioni i paligjshëm;
- Krimi financiar;
- Veprimtaritë e paligjshme të pastrimit të parave;
- Kontrabanda dhe mashtrimi doganor;
- Armët e zjarrit dhe armët e tjera;
- Mjetet motorike të vjedhura;
- Siguria e kontenierëve;
- Falsifikimi i parave dhe mjeteve të pagesës;
- Krimi i lidhur me lëndët bërthamore dhe radioaktive;
- Krimet e lidhura me mjedisin dhe natyrën;
- Krimi kibernetik.

DBPN-ja mund të ndihmojë në kërkesat për informacion dhe zbulim në marrëdhëniet Polici-me-Polici, por këto informacione mund të përdoren vetëm nga Policia. Prokuroria mund ta përdorë këtë instrument për bashkëpunim ndërkombëtar, por

vetëm të dhënat e përftuara nga MLA janë të pranueshme si provë në gjykatë.

Për çdo lloj prove, ku përfshihen: të dhënat e komunikimit (me ose pa kërkesë për ruajtje), informacioni financiar ose informacioni tjetër privat, duhet të bëhet nga prokurori një Kërkesë për Ndihmë Ligjore Reciproke (në kuadër të MLAT) dhe të dorëzohet përmes kanaleve gjyqësore në zonën gjyqësore ku ndodhen informacionet. Në raste urgjente, DBPN-ja mund të ndihmojë në ndjekjen e shpejtë të kërkesës nëpërmjet partnerëve të saj ndërkombëtarë.

DBPN ka një pikë qendrore kontakti për koordinimin e kërkesave për ndihmë ndërkombëtare dhe për identifikimin e partnerit më efektiv ndërkombëtar që mund të ndihmojë në ndjekjen e një denoncimi të dhënë.

DBPN-ja mund të kontaktohet 24 orë, në të gjitha ditët e javës (24/7).

Ekipi i Përbashkët Hetimor (EPH)

EPH është një marrëveshje për ngritjen e një ekipi hetimor për një periudhë të caktuar dhe për një qëllim të caktuar. Qëllimi i EPH-së është hetimi i rasteve specifike dhe mundësimi i një procesi të shpejtë të zbulimit të informacionit dhe të provave përmes bashkëpunimit policor dhe gjyqësor.

EPH-ja mund të ngrihet për një **hetim ndërkombëtar** që përfshin dy ose më shumë vende dhe mund të përbëhet nga agjencitë e Interpolit, SELEC, Europol dhe Eurojust. Për Republikën e Shqipërisë, EPH-ja kryesohet nga prokurori.

Europol

Shqipëria është partnere operacionale e Europolit dhe ka një Byro Ndërlidhëse në Hagë, e cila mund të kontaktohet përmes DBPN-së për të ndihmuar në bashkëpunimin operacional dhe strategjik, që përfshin anëtarët dhe partnerët operacionalë të Europolit.

Eurojust

Eurojust ka marrëveshje me Prokurorinë shqiptare dhe me organe të tjera të BE-së, si me Rrjetin Gjyqësor Evropian, Europol-in dhe OLAF-in. Eurojust ofron bashkëpunim gjyqësor në çështje penale për të përmirësuar adresimin e krimit të rëndë ndërkufitar dhe krimit të organizuar, duke nxitur koordinimin e hetimit dhe bashkëpunimin në nivel prokurorie mes agjencive të Shteteve Anëtare të BE-së dhe partnerëve të bashkëpunimit.

Interpol

Interpol-i (International Criminal Police Organisation) ka 190 vende anëtare. Byroja Qendrore Kombëtare (BQK Tiranë) për Shqipërinë ka akses në gamën e bazave të dhënave kriminale dhe të zbulimit të INTERPOL-it.

SELEC – South East Law Enforcement Center

SELEC ofron mbështetje për Shtetet Anëtare për të rritur koordinimin në parandalimin dhe luftimin e krimit, duke përfshirë krimin e rëndë dhe të organizuar, ku një krim i tillë përfshin ose duket se përfshin një element të aktivitetit ndërkufitar.

Aktivitetet operacionale të SELEC kryhen në kuadër të tetë Task Forcave (TF) që trajtojnë çështjet e 12 shteteve anëtare të SELEC, që janë: Republika e Shqipërisë, Bosnja dhe Hercegovina, Republika e Bullgarisë, Republika e Kroacisë, Republika e Maqedonisë së Veriut, Republika e Greqisë, Hungaria, Republika e Moldavisë, Mali i Zi, Rumania, Republika e Serbisë dhe Republika e Turqisë.

Njësia e Ndjekjeve – (Të arratisurit)

Njësia e Ndjekjeve përpiqet të identifikojë personat e kërkuar në nivel kombëtar ose ndërkombëtar. Ata kanë, gjithashtu, autoritetin për të ndjekur të arratisurit e kërkuar përmes operacioneve të orientuara ndaj objektivave.

Relevanca: Hetimet Kompjuterike

Partnerët Kombëtarë

Sektori i Menaxhimit të Incidenteve Kibernetike i AKCESK/NAECCS

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është ngritur dhe përbën pikën zyrtare kombëtare të kontaktit dhe koordinimit në trajtimin e incidenteve të sigurisë në rrjetet dhe sistemet e informacionit, si dhe identifikon e reagon ndaj incidenteve dhe rreziqeve të sigurisë kompjuterike.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka misionin e mëposhtëm:

a. koordinon dhe ndihmon/asiston autoritetet dhe institucionet e sektorit publik në implementimin e shërbimeve proaktive për uljen e rrezikut të incidenteve të sigurisë kompjuterike, si dhe në trajtimin e incidenteve kur ato ndodhin;

b. zhvillon aktivitete për edukimin dhe ndërgjegjësimin e qytetarëve për efektet negative të kërcënimeve kompjuterike dhe të krimit kompjuterik;

c. siguron mbështetje për të gjitha institucionet e saj anëtare, përfshirë edhe Ministrinë e Brendshme.

Për më shumë informacion shihni www.cesk.gov.al/

Sektori i Hetimit Financiar dhe Sektori i Zbulimit Financiar

Sektori i Zbulimit Financiar është organ në kuadër të Ministrisë së Financave të Republikës së Shqipërisë dhe, së bashku me Sektorin e Hetimit Financiar, ka autorizime të posaçme në zbatim të Ligjit për Procedurën Penale, ku përfshihen:

- kryerja e hetimeve paraprake dhe mbledhja e provave për krimin e organizuar financiar dhe ndjekjen e gjurmëve të parave në shuma të konsiderueshme, për të gjetur autorin, për të parandaluar fshehjen apo arratisjen e autorit apo bashkëpunëtorit, si dhe për të mbledhur të gjitha informacionet që mund të jenë të dobishme për zhvillimin e procedurës penale;
- kryerja e analizave kompjuterike të sendeve të konfiskuara, informacioneve kompjuterike ose të dhënave nga pajisje të tjera elektronike dhe mekanike që përmbajnë informacion, të cilat mund të shërbejnë si provë gjatë kryerjes së procedurave hetimore paraprake;
- mbështetja e organeve dhe institucioneve të tjera qeveritare, duke përgatitur dhe paraqitur gjetjet dhe mendimet e ekspertëve brenda kompetencës së tij;
- bashkëpunimi me organe homologe nga vende të tjera, në përputhje me marrëveshjet dypalëshe dhe marrëveshjet ndërkombëtare të ratifikuara.

Në lidhje me krimin kompjuterik, të dyja njësitë mund të ndihmojnë në mënyrë specifike në hetimet kibernetike, si “gjurmimi i parave” nëpërmjet shërbimeve të pagesave në internet si PayPal dhe në raste të tjera komplekse mashtrimi.
Kërkesat për ndihmë duhet të drejtohen përmes prokurorisë.

TË DHËNAT NGA BURIME TË HAPUR (OSINT) – VËSHTRIM I PËRGJITHSHËM

Hulumtimi dhe hetimi në internet është një mjet i fuqishëm kundër krimit. Ai, gjithashtu, paraqet sfida të reja për zbatimin e ligjit, pasi përdorimi i një mjeti të tillë ende mund të ndërhyjë në të drejtën e një personi për respektimin e jetës private dhe familjare, e cila parashikohet në nenin 8 të Ligjit për të Drejtat e Njeriut 1998 dhe KEDNJ.

Autoritetet publike duhet të sigurojnë që çdo ndërhyrje në këtë të drejtë është:

- e nevojshme për një objektiv specifik dhe legjitim – siç është parandalimi ose zbulimi i krimit;
- në përpjesëtim me objektivin në fjalë;
- në përputhje me ligjin.

Sa herë që përdorim Internetin për të mbledhur të dhëna ose prova, duhet të kemi parasysh se mund të ndërhyjmë në të drejtën e një personi për respektimin e jetës private dhe familjare dhe, nëse po, atëherë duhet të kërkojmë autorizim sipas KPP dhe duhet të informohet prokuroria. Në këtë udhëzues janë përcaktuar parimet që do t'ju ndihmojnë të identifikoni nëse është i përshtatshëm një autorizim i tillë.

Është gjithashtu thelbësore të merret në konsideratë efekti i çdo ndërhyrjeje kolaterale në jetën private dhe familjare të njerëzve të tjerë, që nuk lidhen drejtpërdrejt me subjektin e kërkimit ose hetimit. Gjykimi rast pas rasti është jetik kur hulumtoni ose hetoni në internet.

Vështrim i përgjithshëm

- Komunikimi online nëpërmjet internetit është bërë vitet e fundit metodë e preferuar e komunikimit me individë të tjerë, brenda grupeve sociale apo me këdo në botë me akses në internet. Një komunikim i tillë mund të përfshijë faqet e internetit, rrjetet sociale, dhomat e bisedave (chat rooms), rrjetet e informacionit (p.sh. Facebook/Twitter) dhe/ose postën elektronike të bazuar në web.
- Vetëm për faktin se edhe njerëzit e tjerë mund ta shohin informacionin, kjo nuk do të thotë patjetër se një person nuk kërkon privatësi në lidhje me informacionin e postuar në internet.
- Përdorimi i teknikave të fshehta për të vëzhguar, monitoruar dhe marrë informacion privat mund të çojë në ndërhyrje në të drejtën e një personi

për respektimin e jetës private dhe familjare, kështu që është thelbësore siguria që një veprim i caktuar hetuesve është i ligjshëm dhe i autorizuar.

Konsideratat për rrezikun operacional

- Çdo kërkim dhe hetim në internet lë "gjurmë". Prandaj, do të duhet të merret një vendim operacional nëse dëshironi të siguroheni që kërkimi juaj është i pa-atribueshëm, pra nuk mund të gjurmohen organet e zbatimit të ligjit ose individët e identifikueshëm, apo nëse dëshironi që kërkimi të mund të atribuohet, pra të gjurmohet për të arritur tek forcat e rendit.
- Hulumtimi dhe hetimi i pagjurmueshëm duhet të kryhen me pajisje që nuk mund t'i atribuohen organeve të zbatimit të ligjit ose individëve të identifikueshëm. Përdorimi i pajisjeve që i atribuohen atyre rrezikon të kompromet ojë çdo aktivitet operacional që është kryer në të.
- Rekomandohet që kërkimi dhe hetimi i gjurmueshëm të kufizohen në zonat e kërkimit të aksesueshme nga publiku, p.sh. hartat, pamjet e rrugëve, faqet e autoriteteve lokale, faqet e ankandeve, etj. dhe faqet e internetit, në të cilat nuk është e nevojshme të regjistrosh detaje për të pasur akses.
- Dihet që shumë oficerë dhe staf kanë përvojë të konsiderueshme në përdorimin e internetit për kërkimet e tyre personale në internet. Megjithatë, drejtuesit duhet të garantojnë që personeli që kryen kërkime dhe hetime online për Policinë Shqiptare të jetë kompetent dhe i trajnuar siç duhet.

Siguria

Kur ndërmerren kërkime dhe hetime në internet, duhet t'i kushtohet vëmendje:

- Burimit të duhur për blerjen e pajisjeve për përdorim të fshehtë.
- Veçimit të pajisjeve të përdorura për aktivitet të fshehtë nga ato për aktivitet të hapur.
- Sigurimit që pajisjet e përdorura për veprimtari të fshehtë nuk mund të gjurmohen deri tek zbatuesit e ligjit.
- Si, dhe ku, të kapni, regjistroni dhe ruani plotësisht informacionin e marrë online.
- Si, dhe ku, të regjistrohen veprimet e personit që kryen kërkimin ose hetimin, në mënyrë që të jetë më pas i audituesshëm.

- Metodave të preferuara të prodhimit të dhënave në formë prove.

Përdorimi i pseudonimit

- Krijimi i një pseudonimi për qëllime të hetimit penal duhet të autorizohet nga prokurori, sipas masave të posaçme hetimore në KPP.
- Dihet se, për kërkime dhe hetime të fshehta në internet, duhet një kërkesë për krijimin dhe përdorimin e një llogarie (account) në emrin e pseudonimit të krijuar me qëllim mbledhjen e informacioneve të nevojshme. Ndërkohë, mund të ndërmerret krijimi i një pseudonimi për kërkim online, por informacioni i marrë nuk mund të përdoret si provë. Megjithatë, kjo mund të çojë në shkelje të termave dhe kushteve të disa faqeve, veçanërisht të rrjeteve sociale.
- Pseudonimet duhet të përdoren vetëm për kërkime dhe hetime të fshehta që duhet të ndërmerren duke përdorur një kompjuter, identiteti i të cilit nuk mund t'i atribuohet asnjë personi apo vendi.
- Duhet të mbahet nga policia një regjistër i të gjitha profileve të personave të krijuar dhe të përdorur si llogari. Ky regjistër duhet të mbahet në qendër dhe duhet të rishikohet periodikisht, duke marrë parasysh se sa e domosdoshme dhe sa proporcionale është mbajtja dhe përdorimi i çdo pseudonimi të regjistruar.
- Për çdo përdorim të një pseudonimi duhet të mbahet një regjistër, ku regjistrohet ora, data, përdoruesi dhe qëllimi për të cilin është përdorur pseudonimi.

Burimet e hapura

- Shumica e informacioneve të disponueshme në internet mund të gjendet nga kushdo që ka akses në internet, qoftë falas apo me pagesë. Këto informacione njihen gjerësisht si informacion me burim të hapur.
- Shikimi i informacionit me burim të hapur, qoftë me mjete të atribueshme ose të pa-atribueshme, nuk përbën marrje të informacionit privat, sepse ai informacion është i disponueshëm publikisht. Nëse informacionet janë të hapura për publikun, ose janë të disponueshme publikisht, nuk konsiderohen më si të dhëna personale. Për shembull, nëse një person i bën të hapura për publikun fotot nga llogaria e vet në Facebook, këto nuk janë më të dhëna personale.

- Sipas neneve të masave të posaçme hetimore në KPP, prokurori duhet të njoftohet që në fillim të hetimit.
- Regjistrimi, ruajtja dhe përdorimi i informacionit me burim të hapur, për të krijuar një profil të një personi ose një grupi njerëzish, duhet të jetë i nevojshëm dhe proporcional dhe, për të garantuar që çdo ndërhyrje në të drejtën e një personi për respektimin e jetës private dhe familjare është e ligjshme, ai duhet të ruhet dhe përpunohet në përputhje me parimet e legjislacionit të të dhënave.

Informacioni me akses të kufizuar

Qasja në disa nga informacionet në internet është e kufizuar nga "pronari". Një formë e zakonshme kufizimi i kësaj natyre haset në rrjetet sociale, ku pronari një profili mund të përdorë cilësimet e privatësisë për të kufizuar aksesin te "miqtë" në internet. Për të parë në mënyrë të fshehtë informacionin me akses të kufizuar, prokurorisë **do t'i duhet** urdhër gjykate.

Konsiderata ligjore

Teknikat e kërkimit dhe të hetimit në internet mund të kenë ndikim në të gjitha sa vijon në të njëjtën kohë ose në një prej tyre:

- Përgjimin e komunikimeve dhe marrjen e të dhënave të komunikimit
- Burimet Njerëzore të Zbulimit që përdoren për Survejim dhe Infiltrim
- Keqpërdorimin e kompjuterit
- Mbrojtjen e të dhënave
- Të drejtat e njeriut/Konventa Evropiane për të Drejtat e Njeriut - Të dyja këto ofrojnë një sërë të drejtash themelore, të cilat janë thelbësore për të gjitha veprimet në zbatim të ligjit.

E drejta, e cila ka më shumë mundësi të preket nga oficerët dhe stafi që ndërmarrin kërkime dhe hetime në internet, është e drejta sipas nenit 8 të Konventës Evropiane për të Drejtat e Njeriut, i cili thotë:

- 8.1 Çdokush ka të drejtën e respektimit të jetës së tij private dhe familjare, banesës dhe korrespondencës së tij.
- 8.2 Autoriteti publik nuk mund të ndërhyjë në ushtrimin e kësaj të drejte, përveçse në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes të sigurisë publike, për mbrojtjen

e rendit publik, shëndetit ose moralit, ose për mbrojtjen e të drejtave dhe lirive të të tjerëve.

Veprimtaritë në vijim mund të përbëjnë shkelje të legjislacionit për krimin kompjuterik:

- përdorimi i emrit të përdoruesit dhe fjalëkalimit të një personi tjetër pa autorizim të ligjshëm për të hyrë në të dhëna ose në një program;
- ndryshimi, fshirja, kopjimi apo heqja e një programi ose të dhënave;
- imitimi i një personi tjetër, duke i përdorur e-mailin, duke bërë chat online ose përdorur shërbime të tjera të bazuara në web.

Prokuroria

- Masat e posaçme hetimore të KPP-së, prokuroria vihet në dijeni për një hetim.
- Masat e posaçme hetimore të KPP-së, marrja e autorizimit nga prokuroria për përdorimin e pseudonimit.

Konsiderata praktike për hetimet mbi të dhënat nga burime të hapura

Për kryerjen e çfarëdolloj hetimi, duhet të dimë parametrat me të cilat veprojmë, por metodologjia ka një aspekt dinamik dhe si hetues ne shpesh "mendojmë jashtë kutisë", pra përtej mënyrave konvencionale, për marrjen e provave.

Megjithatë, kur kryeni investigime në internet, apo çfarëdolloj investigimi, informacioni i disponueshëm është aq i gjerë saqë mund të shpërqendroheni lehtë ose t'i largoheni aktivitetit që synoni të hetoni, prandaj është e domosdoshme që të identifikoni, që në fillim, pikat që do të provoni dhe të keni një plan të strukturuar për kërkimin; që të regjistroni gjurmën e çdo veprimi që kryeni në funksion të auditimeve të mëvonshme dhe për qëllime të vendimmarrjes suaj, si dhe të ruani kopje të asaj çka gjendet, në format elektronik ose në letër, që është relevante për hetimin.

Gjurma e auditimit të metodologjisë së kërkimit OSINT duhet të ketë detaje të mjaftueshme për t'i mundësuar Prokurorit arritjen në të njëjtin përfundim.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale përfshirë Mashtrimet, Kërkimet mbi Adresat IP dhe Domenet

KRIMET KOMPJUTERIKE DHE KRIMET E MUNDËSUARA NGA KOMPJUTERI

Krimi kompjuterik

Krim kompjuterik është çdo veprimtari kriminale që përfshin një kompjuter, pajisje të lidhur në rrjet, apo një rrjet. Shumica e krimeve kompjuterike kryhen me qëllime përfitimi për kriminelët kompjuterikë. Disa krime kompjuterike kryhen drejtpërdrejt kundër kompjuterave apo pajisjeve për t'i dëmtuar apo çaktivizuar ato. Të tjera përdorin kompjutera apo rrjete për të përhapur programe keqdashëse, informacione të paligjshme, imazhe apo materiale të tjera. Disa krime kompjuterike i bëjnë të dyja – pra, vënë në shënjestër kompjutera për t'i infektuar me një virus kompjuterik, i cili më pas shpërndahet në makina të tjera dhe, me raste, në rrjete të tëra.

Një efekt parësor i krimit kompjuterik është ai financiar. Krimi kompjuterik mund të përfshijë shumë tipe të ndryshme veprimtarish kriminale të drejtuara nga përfitimet. Kriminelët kompjuterikë mund të vënë në shënjestër informacionin privat të një individi apo të dhëna ndërmarrjesh për t'i vjedhur dhe rishitur. Përveç rasteve klasike të krimeve kompjuterike, identifikojmë edhe veprimtari të tjera kriminale që lidhen me përdorimin e pajisjeve kompjuterike dhe na duhet të kemi mekanizmat e duhur për të hetuar dhe mbledhur provat elektronike:

Krimet e Mundësuara nga Kompjuterat

Këto janë vepra penale të cilat nuk varen nga kompjuterat apo rrjetet, por që kanë ndryshuar në shkallë apo formë në sajë të përdorimit të Internetit dhe teknologjive të komunikimit. Ato ndahen në kategoritë e mëposhtme:

- Krime kompjuterike që lidhen me ekonominë, përfshirë:
  - Mashtrimet
  - Veprat penale ndaj pronësisë intelektuale – pirateria dhe falsifikimi
- Tregjet online për artikuj të paligjshëm
- Komunikimet keqdashëse dhe fyese, përfshirë:
  - Komunikimet e dërguara përmes mediave sociale
  - Bullizmi kibernetik
  - Mobbing virtual
- Shkelje që synojnë posaçërisht individë të caktuar, përfshirë këtu dhunën ndaj grave dhe vajzave të mundësuar nga kompjuterat:

- Nxjerrja haptas e imazheve seksuale private pa miratim
- Përndjekja dhe ngacmimet me bazë kompjuterike
- Shtrëngimi dhe kontrolli

- Veprat seksuale ndaj fëmijëve dhe imazhet e pahijshme të fëmijëve, përfshirë:
  - Abuzimi seksual i fëmijëve
  - Online grooming
  - Imazhet e ndaluara dhe të pahijshme të fëmijëve
- Pornografia e skajshme, botimet e turpshme dhe imazhet e ndaluara

Krimet e Varura nga Kompjuterat

Krimet e varura nga kompjuterat ndahen gjerësisht në dy kategori kryesore:

- Ndërhyrjet e paligjshme në rrjete kompjuterike, të tilla si *hacking*
- Rrëzimi apo ulja e funksionalitetit të kompjuterave dhe hapësirave të rrjeteve, të tilla si programet keqdashëse dhe sulmet me Bllokime të Shërbimeve (DoS) ose Bllokime të Shpërndara të Shërbimeve (DDoS).

Krimet e varura nga kompjuterat kryhen për shumë arsye të ndryshme nga individët, grupet dhe madje shtetet e pavarura. Për shembull:

- Individët ose grupet me aftësi të larta që mund të programojnë dhe shpërndajnë programe për të sulmuar sisteme dhe rrjete kompjuterike, qoftë për të kryer krime, qoftë për të ndihmuar të tjerët që t'i kryejnë ato;
- Individët ose grupet me nivele të larta aftësish, por me qëllime kriminale të nivelit të ulët, për shembull haktivistet protestues;
- Individët ose grupet me nivele të ulëta aftësish, por me aftësinë për të përdorur instrumente kompjuterike të zhvilluara nga të tjerët;
- Grupet e organizuara kriminale;
- Terroristët kibernetikë që synojnë të shkaktojnë ndërprerje dhe pasoja sa më të mëdha;
- Shtetet e tjera dhe grupet e sponsorizuara nga shtetet, të cilat lëshojnë sulme kompjuterike me synimin e mbledhjes së informacionit mbi asete qeveritare, të mbrojtjes kombëtare, ato ekonomike dhe industriale, ose me synim kompromentimin e tyre; dhe
- Të brendshëm apo punonjës me qasje të privilegjuar në kompjutera dhe rrjete.

Pjesa më e madhe e kriminelëve kompjuterikë kanë nivele aftësish relativisht të ulëta, por sulmet e tyre mundësohen gjithnjë e më shumë nga tregjet online kriminale në rritje, të cilat sigurojnë qasje të lehtë në instrumente dhe mjeshtëri të sofistikuara dhe me porosi, duke u lejuar këtyre kriminelëve kompjuterikë të shfrytëzojnë një diapazon të gjerë dobësish.

Shembujt më të përhapur të krimeve kompjuterike

Siguria Kompjuterike është grupi i teknologjive, proceseve dhe praktikave të modeluara për të mbrojtur rrjetat, kompjuterët, programet, të dhënat dhe individët ndaj sulmeve online, dëmtimeve apo hyrjeve të paautorizuara.

Malware është emërtimi i shkurtër në anglisht për programe keqdashëse, pra programe që mund të përdoren për të kompromentuar ose ndërprerë punën e kompjuterëve apo funksionet e veprimtarive në lëvizje të kompjuterëve, për të vjedhur të dhëna, për të anashkaluar kontrollet e hyrjes, apo për t'i shkaktuar dëme kompjuterit ku ndodhen ato. Ky seksion përcakton një sërë tipesh të përhapura programesh keqdashëse, përfshirë këtu viruset, krimbat, trojanët, botet, kitet e përftimit të administrimit, programet përgjuese, sulmet e imitimit dhe helmimit, si dhe inxhinierinë sociale përmes e-mail-it, VOIP dhe pranisë fizike.

Viruset janë një nga shembujt më të njohur të programeve keqdashëse. Ato mund të shkaktojnë keqfunksionim të lehtë të kompjuterëve, por edhe pasoja më të rënda si dëmtimin apo fshirjen e pajisjeve fizike, programeve dhe skedarëve. Janë programe që shumëfishohen vetë dhe përhapen brenda dhe ndërmjet kompjuterëve. Ato kanë nevojë për një "mbartës" (si për shembull skedar, disk apo tabelë Excel-i) në kompjuter, por nuk mund ta infektojnë një kompjuter pa u hapur apo pa u ekzekutuar nga përdoruesit skedari i infektuar.

- Viruset makro prekin skedarë që krijohen kryesisht nga programet të paketës Microsoft Office si Word apo Excel;
- Viruset e sektorëve të ngarkimit fillestar (boot sector virus) ndryshojnë sektorin e ngarkimit fillestar të disqeve të ngurta apo disqeve të tjera;
- Viruset polimorfike (të shumëtrajtshme) ndryshojnë paraqitjen e tyre pas çdo infektimi për të shmangur antiviruset;
- Viruset metamorfike e hartojnë veten nga e para pas çdo infektimi për të shmangur diktimin e tyre.

Krimbat (Worms) janë gjithashtu programe kompjuterike keqdashëse që shumëfishohen vetë, por ato mund të përhapen me shpejtësi dhe në mënyrë

autonome, brenda dhe ndërmjet kompjuterëve, shpesh duke përdorur kontaktet në librin e adresave të Outlook apo duke kërkuar dhe gjetur porta të hapura në makinat e tjera, pa qenë nevoja për mbartës apo veprim nga përdoruesit. Kështu, ndikimi i krimbave mund të jetë më i rëndë se sa ai i viruseve dhe të krijojë shkatërrime në rrjeta të tëra apo të mbingarkojë burimet e rrjetave në masë të madhe. Krimbat mund të përdoren edhe për të instaluar trojanë në sistemet e rrjetave.

Trojanët janë një formë e programeve keqdashëse që shfaqen si programe legjitime, por që krijojnë mundësi për hyrje të paligjshme në një kompjuter. Ato mund të kryejnë funksione si vjedhja e të dhënave pa dijeninë e përdoruesit dhe mund të mashtrojnë përdoruesit duke kryer në dukje një detyrë rutinë, ndërsa aktualisht ndërmarrin veprime të fshehura dhe të paautorizuara.

Një shembull i rëmdomtë trojani është ai ku një kompjuter kompromentohet dhe shndërrohet në bot (robot) që mund të përdoret për të nisur sulme kundër kompjuterëve të tjerë; trojanë të tjerë mund të përdoren për të instaluar në kompjutera programe kontrolli në largësi. Një trojan do të ishte program i dallueshëm në Task Manager.

Kitet e përftimit të administrimit (Rootkit) Për të instaluar një rootkit, sulmuesit i duhet së pari të fitojë hyrje në llogarinë administruese të pajisjes duke shfrytëzuar dobësitë e sistemit apo duke zbuluar një fjalëkalim në sajë të thyerjes së tij apo nëpërmjet inxhinierisë sociale. Rootkit-et u japin mundësi viruseve dhe programeve të tjera keqdashëse që të fshihen duke u maskuar si skedarë të nevojshëm që nuk kontrollohen nga antiviruset.

Rootkit-et nuk janë të dëmshme në vetvete; ato përdoren thjesht për të fshehur programe të tjera keqdashëse, si bote dhe krimba, brenda pjesëve administrative apo bërthamës së sistemit të shfrytëzimit. Ato nuk mund të dallohen nga Task Manager dhe për diktimin e tyre nevojiten mjete të posaçme. Një rootkit mund të regjistrojë ato që shtyp përdoruesi në tastierë ose të kapë sinjalet e sistemit dhe t'i kalojë ato për te programe të tjera, apo të lejojë hyrje në kompjuter nga jashtë. Meqë rootkit-et vihen në veprim që para se të ngarkohet vetë sistemi i shfrytëzimit, ato janë shumë të vështira për t'u diktuar dhe janë po kështu shumë të vështira për t'u hequr.

Bllokimet e shërbimeve (Denial of service - DoS) dhe **Bllokimet e shpërndara të** shërbimeve (Distributed DoS - DDoS) shfrytëzojnë dobësitë në protokollet e komunikimit dhe krijojnë sulme që përmbytin serverat në Internet me kaq shumë kërkesa saqë këta nuk janë më të aftë që të përgjigjen në kohë. Kjo mund të mbingarkojë serverat, duke shkaktuar ngrirjen apo bllokimin e tyre, gjë që u mohon përdoruesve legjitimë qasjen në një faqe apo shërbim.

- Një sulm **bllokimi shërbimi** është një incident në të cilin një përdorues apo organizatë nuk arrin dot të përdorë shërbimet e një burimi që normalisht do të kishin mundësi t'i përdornin.
- Një **bllokim i shpërndarë shërbimi** është një incident ku një grup i madh sistemesh të kompromentuara (me raste i quajtur botnet) sulmojnë një shënjestër të vetme.

Sulmet DoS/DDoS mund t'i shkaktojnë një personi apo kompanie humbje të mëdha në para dhe kohë. Si rregull, humbja e një shërbimi është pamundësia e një shërbimi të veçantë në rrjet, si për shembull e-mail, për të qenë i disponueshëm, apo humbja e pjesshme e të gjitha lidhjeve dhe shërbimeve në rrjet; kjo mund të shkatërrojë programe dhe skedarë në sistemet kompjuterike të prekura dhe, me raste, ndërpritet puna e një apo disa faqeve në Internet.

Forma të zakonshme sulmesh të tilla janë:

Sulme Mbingarkese Kapaciteti (Buffer Overflow Attacks) janë lloji më i shpeshtë i sulmeve DoS; sulmuesit dërgojnë më shumë trafik drejt një adrese rrjeti se sa është vendosur nga programuesit kapaciteti maksimal i të dhënave që mund të dërgohen. Sulmuesi mund të jenë në dijeni që sistemi në fjalë ka një dobësi konkrete që mund të shfrytëzohet për këtë qëllim, ose thjesht të tentojë sulme me idenë që këto ndoshta do të funksionojnë. Shembuj të tillë janë paketat ICMP (Internet Control Message Protocol) me madhësi përtej standardeve – kjo quhet PING-u i vdekjes ("PING of death", nga Packet Internet or Inter-Network Groper - PING)

Sulme sinkronizimi - Kur nis një sesion komunikimi ndërmjet dy pajisjeve që përdorin protokollin TCP (Transport Control Protocol) në rrjet, krijohet fillimisht një hapësirë shumë e vogël për "shtrëngimin e duarve", një proces zakonisht shumë i shpejtë për çeljen e sesionit. Paketat e çeljes së sesionit përfshijnë një fushë SYN që identifikon renditjen në shkëmbimin e mesazheve. Një sulmues mund të dërgojë një sasi të madhe kërkesash për lidhje, dhe/ose me shpejtësi tepër të lartë, dhe më pas të mos kthejë përgjigje rikonfirmuese. Meqë hapësira e rezervuar për qëllimin e çeljes së komunikimit është e paktë, mbetja e paketës së parë pa përgjigje shkakton që kërkesat e tjera, legjitime, për lidhje të mos përfillen. Ndonëse një paketë hidhet tej nëse ka mbetur pa përgjigje përtej një afati të caktuar, një numër i madh kërkesash për lidhje të lëna përgjysmë e bën të vështirë çeljen e sesioneve të kërkuara në mënyrë legjitime dhe të rregullt.

Sulme fragmentimi (Teardrop Attack) shfrytëzon faktin që Protokolli i Internetit (IP - Internet Protocol, një nga protokollet e komunikimit që përdoren në Internet e rrjeta të tjera) kërkon që një paketë tepër e madhe për ruterin e radhës të ndahet

në fragmente. Secili fragment i paketës identifikon një vlerë diference me fillimin e paketës së parë, gjë që e lejon të tërë paketën që të ribashkohet nga sistemi marrës. Në një sulm fragmentimi, mënyra e zbatimit të IP nga sulmuesi vendos te paketa e dytë, apo e tretë, etj. një vlerë diference që e ngatërron sistemin marrës dhe e bën që të bllokohet.

Sulme me Përgjigje të Shumëfishta (Smurf Attack) Në këtë lloj sulmi dërgohet një kërkesë pingimi (e quajtur echo) te një sistem marrës, paketë në të cilën është përcaktuar që ajo duhet të shpërndahet te një numër makinash brenda rrjetit lokal të sistemit marrës dhe në të cilën origjina e saj reale është zëvendësuar me atë të sistemit të sulmuar. Si rezultat, do të kthehen kaq shumë përgjigje nga ato makina të tjera për te sistemi marrës (në vend të sistemit dërgues), saqë ai nuk do të jetë më në gjendje që të marrë apo dallojë trafikun që vjen nga burime reale.

Sulme me Shpërndarje të Shumëfishtë (Fraggle Attack) është një sulm që përfshin dërgimin e një sasie të madhe trafiku UDP të manipuluar drejt adresës shpërndarëse të një ruteri brenda rrjetit. Është sulm shumë i ngjashëm me ato me përgjigje të shumëfishta.

(Meqë ruterat nuk përcjellin më paketa që drejtohen te adresat shpërndarëse, shumica e rrjeteve janë të mbrojtura nga sulmet me përgjigje të shumëfishta apo me shpërndarje të shumëfishtë.)

Relevanca: Hetimet mbi Krimet Kompjuterike, Sulmet Kibernetike, Infrastruktura Kritike Kombëtare

Portat e Pasme (Backdoors) janë shërbime në linjë apo porta të hapura që i lejojnë një përdoruesi në largësi që të lidhet dhe të anashkalojë mekanizmat standardë të autentikimit në kompjuter. Portat e pasme siç janë programi ndihmës Netcat lejojnë lidhje në largësi gjatë të cilave një përdorues keqdashës mund të bëjë në kompjuter çdo gjë që dëshiron dhe ndërkohë përdoruesi përballë pajisjes nuk e dallon qasjen që po ndodh nga jashtë. Portat e pasme përdoren nga ndërhyrësit e paautorizuar për të pasur mundësi që të kthehen përsëri te një kompjuter pasi të kenë përftuar qasje më parë.

Sulmet për shpërblesë (Ransomware) janë forma të veprimtarive keqdashëse në të cilat skedarët lokalë në kompjuterin tuaj bllokohen dhe qasja tek ta bëhet e pamundur; kjo pasohet nga një kërkesë pagese për çbllokim, duke përdorur ndonjë metodë pagese të pagjurmueshme (si për shembull Bitcoin).

Bomba logjike (Logic bomb) është një program keqdashës i kurdisur që të dëmtojë në një moment të caktuar, por që nuk aktivizohet deri atëherë. Një "shkrehës" i caktuar, si për shembull një datë dhe orë e programuar që më parë,

aktivizon *bombën logjike* dhe ekzekuton kod keqdashës që i shkakton dëme një kompjuteri apo një rrjeti.

Rrjet botesh (Botnet) është emri që i jepet një numri kompjuterash në Internet që, ndonëse pronarët e tyre nuk janë në dijeni, janë kompromentuar dhe përdoren për të përcjellë transmetime (përfshirë këtu sulme DoS, spam apo viruse) te kompjutera të tjerë në Internet. Secilit prej një kompjuteri të tillë i referohet si zombi, kompjuter "robot", apo shkurt bot. Shumica e kompjuterave të kompromentuar në këtë mënyrë janë nëpër banesa dhe mund të jenë me dhjetëra mijëra. Kompjuterët që formojnë një botnet mund të programohen që të drejtojnë transmetime drejt kompjuterave specifikë, të tillë si një faqe e caktuar që sulmohet për ta mbyllur për publikun; ky njihet si sulm bllokues i shpërndarë (DDoS).

Regjistruesi i tastave (Keylogger) është një lloj programi përgjues që ka aftësinë të regjistrojë në një skedar regjistrimi, zakonisht të shifruar, çdo shtypje taste në tastierë. Një regjistrues tastash mund të ruajë mesazhe chat-i, e-maile dhe çdo informacion tjetër që futet në kompjuter nga tastiera. Ai mund të jetë program i instaluar në kompjuter apo një pajisje fizike që lidhet ndërmjet tastierës dhe kompjuterit.

Programet e përgjimit (Spyware) janë programe që sulmojnë privatësinë e përdoruesve në sajë të mbledhjes së informacionit sensitive apo personal nga sistemet e infektuara dhe i transmetojnë ato te palë të treta. Programet e përgjimit mund të fshihen brenda programeve që nxjerrin reklama dhe mund të kapin pamje ekrani nga kompjuterët e përdoruesve.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale përshirë Mashtrimet, Reverse Engineering of Malware.

Inxhinieria Sociale (Social Engineering) është sulmi që shfrytëzon tipare të sjelljes dhe natyrës njerëzore – "ndërhyrja e paautorizuar te njerëzit". Individët nxiten nëpërmjet e-mailit, telefonit, në takime ballë për ballë, apo nëpërmjet imitimit të personave të tretë, që të japin informacion personal. Nëpërmjet procesit të bindjes që identiteti i sulmuesit është ai i një administrator sistemi, inxhinieri apo tekniku që po u bën një shërbim, ata nxiten që të tregojnë informacion për kode hyrjeje, sekrete tregtare, të dhëna personale apo hollësi financiare duke u nisur nga histori të besueshme.

Kërcënimet kompjuterike nëpërmjet Email

Më poshtë vijojnë tipe specifike të kërcënimeve kompjuterike që kryhen nëpërmjet përdorimit të postës elektronike, në situata si rastësore ashtu edhe të synuara.

Spam është mesazh i padëshiruar dhe i pakërkuar i ardhur me e-mail, zakonisht i shpërndarë njëherësh te një numër i madh marrësish në gjithë botën dhe shpesh lidhet me produkte farmaceutike apo me pornografinë. Email-et spam përdoren edhe për të dërguar email-e me bazë shtirjeje (lexo më poshtë) apo programe keqdashëse dhe mund t'i ndihmojnë kriminelët që të arrijnë fitime maksimale.

Email me bazë shtirjeje (Phishing) është një formë mashtrimi në të cilën një sulmues përpiqet të marrë informacion të tillë si kode hyrjeje apo të dhëna llogarish duke u shtirur si një person apo ent i besueshëm në kanale komunikimi elektronik si email, mesazhe të çastit etj. Zakonisht, një viktimë merr mesazh që duket sikur vjen nga një kontakt i mëparshëm apo nga një organizatë e njohur. Një bashkëlidhje apo linqet në e-mail mund të instalojnë programe keqdashëse në pajisjen e lexuesit apo ta drejtojnë atë te një faqe keqdashëse e ngritur posaçërisht për t'i kërkuar atij informacion personal dhe financiar, siç janë fjalëkalimet, numrat identifikues të llogarive apo të dhëna të kartave të kreditit. Variante të tjera përfshijnë:

- Email-et Phishing të synuara janë një variant që synon individë apo grupe të veçanta brenda një organizate, me qëllim përftimi të informacioneve personale.
- Whaling është praktika e dërgimit të email-eve të shtirura te audienca të synuara në nivel të lartë ose të mesëm drejtues në një organizatë (menaxherë, drejtorë etj.)
- Vishing përdor rrjetet digjitale VoIP për të bërë telefonata të pakërkuara me qëllim përftimi informacioni.
- Spim është një variant i spam në të cilin përdoren mesazhet e çastit (në chat etj.) për të dërguar mesazhe të padëshiruara.
- Smishing është variant i phishing që përdor SMS.

Falsifikimi i Kokës së Email është ndryshimi i kokës së një email-i në mënyrë që mesazhi të duket sikur e ka origjinën nga një person apo vendndodhje të ndryshme nga ajo aktualja.

Email-et me rrengje i nxitin përdoruesit që të kryejnë veprime që mund të dëmtojnë kompjuterin, por që janë tërësisht të panevojshme.

Doxing është praktika e kërkimit, zbulimit dhe shpërndarjes gjerësisht të informacionit personalisht identifikues për një individ, duke përdorur baza të dhënash publike, faqe mediash sociale, ndërhyrje të paautorizuara dhe inxhinieri sociale.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale përshirë Mashtrimet...

Kërcënimet kompjuterike me natyrë fizike

Përveç inxhinierisë sociale, ekzistojnë edhe kërcënime të tjera me natyrë fizike që krijojnë rreziqe kompjuterike nëpërmjet përfshirjes së pranisë njerëzore ose regjistrimeve elektronike, si video.

Përgjimi pas shpine është vështrimi nga mbrapa një personi që po vendos një fjalëkalim në kompjuter apo numrin e tyre PIN në bankomat, ose format që krijojnë me gisht në ekranet e hyrjes në mjedise të siguruara.

Gërmimi në kazanë – procesi i hulumtimit në koshat e plehrave dhe kazanët e mbeturinave për të zbuluar informacion të vlefshëm, dokumente të hedhura, shënime në copa letre etj. Një burim tjetër i dobishëm është koshi i letrave pranë printerit.

Grabitja e Identitetit është krim në të cilin dikush përfton pjesë kyçe informacioni personal, të tilla si llogari email-i, profile në media sociale apo llogari bankare me qëllim që të shtiret si dikush tjetër. Informacioni mund të përdoret për të marrë kredi, mallra dhe shërbime në emër të viktimës, apo për t'i siguruar grabitësit kredenciale të rreme.

Mashtrimi me kartat e pagesave është një term i gjerë për grabitjen dhe mashtrimet e kryera me, apo që përfshijnë, karta pagesash të tilla si kartat e kreditit apo debitit, si burim i padrejtë fondesh gjatë një transaksioni. Qëllimi mund të jetë përftimi i mallrave pa paguar apo tërheqja e paautorizuar e fondeve nga një llogari.

Rezervimi i padrejtë i domeneve (Cybersquatting) është regjistrimi, trafikimi apo përdorimi i domeneve me qëllim përfitimi nga një emër i njohur apo markë tregtare që i përket dikujt tjetër. Ky krim mund të ketë lidhje me piraterinë e programeve informatike, shkeljet e të drejtës së autorit dhe dhunimet e markave të regjistruara.

Mallrat dhe Shërbimet e Rreme Shumica e njerëzve i shoqërojnë mallrat e rreme me veshjet, muzikën dhe filmat; një sërë mallrash në përdorim të përditshëm si medikamentet dhe pjesët e makinave riprodhohen në mënyrë të paligjshme dhe me cilësi aq të dobët saqë mund të jenë të dëmshme për publikun.

Qasja në këto mallra mund të arrihet me raste me anë të blerjeve në faqet apo ankandet online, por një numër në rritje po ofrohet nëpërmjet faqeve mashtruese dhe email-eve që përmbajnë linqe për te faqe apo reklama mashtruese. Këto faqe dhe linqe shpesh janë të ngarkuara me programe keqdashëse, me qëllim pengimin e veprimeve normale të një kompjuteri apo pajisjeje të lëvizshme apo grabitjen e të dhënave personale dhe financiare të një përdoruesi.

Shërbimet e pagesave që shoqërohen me këto faqe janë shpesh legjitime, por informacioni personal që dorëzohet në këto faqe mblidhet dhe më pas përdoret nga, apo shitet te, rrjetet kriminale për qëllime mashtrimi.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale, Skimming, Siguria Publike

Sulmet me Falsifikime dhe Helmime

Një sulm me falsifikime ndodh kur një palë imiton me qëllim të keq një pajisje ose përdorues tjetër në rrjet; për të nisur sulme kundër pajisjeve të rrjetit, për të vjedhur të dhëna, për të përhapur programe keqdashëse apo për të anashkaluar kontrollet e hyrjes. Ekzistojnë lloje të ndryshme të sulmeve me falsifikime që mund të përdoren nga palët keqdashëse për ta arritur këtë. Disa nga metodat më të zakonshme përfshijnë sulmet me falsifikime të adresave IP, atyre të adresave ARP dhe atyre të serverave DNS.

Sulmet me Falsifikime të Adresave IP

Maskimi i adresave IP është një nga metodat më të përdorura të sulmit me falsifikime. Në një sulm me falsifikim adrese IP, një sulmues dërgon paketa IP nga një adresë burimore e rreme ose “e maskuar” në mënyrë që të fshihet. Sulmet e bllokimit të shërbimeve (DoS) shpesh përdorin falsifikimin e adresave IP për të mbingarkuar rrjetet dhe pajisjet me paketa që duket sikur vijnë nga adresa IP legjitime.

Ka dy mënyra për të përdorur sulmet e falsifikimit të IP-së për të mbingarkuar objektivat me trafik. Një metodë është thjesht përmbytja e një objektivi të zgjedhur me paketa nga adresa të shumta të falsifikuara. Kjo metodë funksionon duke i dërguar drejtpërdrejt viktimës më shumë të dhëna sesa mund të përpunojë. Metoda tjetër është të falsifikohet adresa IP e objektivit dhe të dërgohen paketa nga ajo adresë për te shumë marrës të ndryshëm në rrjet. Kur një makinë tjetër merr një paketë, ajo automatikisht do t’i transmetojë një paketë dërguesit si përgjigje. Meqenëse paketat e falsifikuara duket se dërgohen nga adresa IP e

objektivit, të gjitha përgjigjet ndaj paketave të falsifikuara do të dërgohen te (dhe do të vërshojnë për te) adresa IP e objektivit.

Sulmet e falsifikimit të IP-së mund të përdoren gjithashtu për të anashkaluar verifikimet e bazuar në adresën IP. Ky proces mund të jetë shumë i vështirë dhe përdoret kryesisht kur ekzistojnë marrëdhënie besimi midis makinave në një rrjet dhe sistemeve të brendshme. Marrëdhëniet e besimit përdorin adresat IP (në vend të kredencialeve të përdoruesve) për të verifikuar identitetet e makinave kur përpiqen të hyjnë në sisteme. Kjo u mundëson palëve keqdashëse të përdorin sulme falsifikimi për të imituar makinat me leje aksesi dhe për të anashkaluar masat e sigurisë së rrjetit të bazuara në besim.

Sulmet e falsifikimit të ARP ndodhin kur një palë keqdashëse dërgon mesazhe të falsifikuara ARP nëpër një rrjet lokal në mënyrë që adresa MAC e sulmuesit të lidhet me adresën IP të një pjesëtari legjitim të rrjetit. Ky lloj sulmi falsifikimit bën që të dhënat e synuara për adresën IP të viktimës t'i dërgohen sulmuesit. Palët keqdashëse zakonisht përdorin falsifikimin e ARP për të vjedhur informacione, për të ndryshuar të dhënat në tranzit ose për të ndaluar trafikun në një LAN. Sulmet e falsifikimit të ARP-së mund të përdoren gjithashtu për të lehtësuar lloje të tjera sulmesh, duke përfshirë bllokimin e shërbimeve, rrëmbimin e sesioneve dhe sulmet me ndërhyrës të ndërmjetëm. Falsifikimi i ARP funksionon vetëm në rrjetet lokale që përdorin Protokollin e Zgjidhjes të Adresave (ARP).

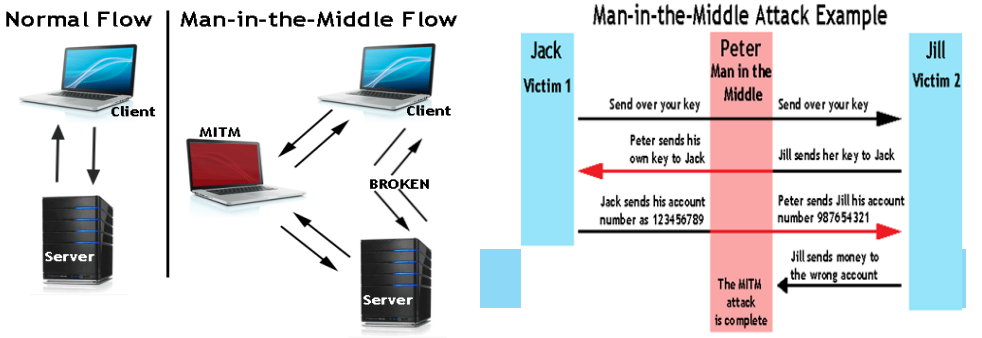
Sulmet e helmimit ARP - të njohura gjithashtu si helmimi i kujtesës (cache) të ARP ose drejtimi i helmit të ARP është një formë sulmi në të cilën një sulmues ndryshon adresën e Kontrollit të Qasjes në Media (MAC) dhe sulmon një LAN Ethernet duke ndryshuar kujtesën ARP të kompjuterit objektiv me një kërkesë dhe përgjigje të falsifikuar ARP dhe paketa përgjigjeje. Kjo zëvendëson adresën MAC të shtresës Ethernet me adresën MAC të njohur të ndërhyrësit të paautorizuar për qëllime monitorimi. Për shkak se përgjigjet ARP janë të falsifikuara, kompjuteri objektiv ia dërgon pa dashje kornizat e paketave fillimisht kompjuterit të ndërhyrësit të paautorizuar në vend që t'i dërgojë në destinacionin origjinal. Si rezultat, kompromentohen të dhënat dhe privatësia e përdoruesit. Një përpjekje efektive për helmim të ARP-së është e pazbulueshme për përdoruesit.

Një sulmues përdor procesin e falsifikimit të ARP për të "helmuar" tabelën ARP të një viktime, në mënyrë që ajo të përmbajë çiftime të gabuara ose të ndryshuara të adresave IP me ato MAC për sulme të ndryshme, të tilla si sulmet me ndërhyrës të ndërmjetëm.

Sulmet e falsifikimit të serverave DNS ndodhin kur një palë keqdashëse modifikon serverin DNS në mënyrë që të ridrejtojë një emër domeni specifik te një adresë IP e ndryshme. Në shumë raste, adresa IP e re do të jetë për një server

që aktualisht kontrollohet nga sulmuesi dhe përmban skedarë të infektuar me programe keqdashëse. Sulmet e falsifikimit të serverave DNS shpesh përdoren për të përhapur krimbat dhe viruset kompjuterike.

Sulmet Me Ndërhyrës të Ndërmjetëm (Man-in-the-Middle) janë një lloj sulmi kibernetik ku një aktor keqdashës futet në një bisedë mes dy palëve, imiton të dyja palët dhe fiton akses në informacionin që të dy palët përpiqen t'i dërgojnë njëra-tjetrës. Një sulm me ndërhyrës të ndërmjetëm i lejon një aktori keqdashës të përgjojë, dërgojë dhe marrë të dhëna të destinuara për dikë tjetër, ose që nuk synohet të dërgohen fare, pa e ditur asnjëra palë e jashtme derisa të jetë tepër vonë. Emri i këtyre sulmeve mund të shkurtohet në shumë mënyra, duke përfshirë MITM, MitM, MiM ose MIM.



Shembuj të sulmeve me ndërhyrës të ndërmjetëm

Në shembullin e parë, sulmuesi e fut veten në mes të fluksit të trafikut ndërmjet klientit dhe serverit. Tani që sulmuesi ka ndërhyrë në komunikimin midis dy pikave fundore, ai/ajo mund të injektojë informacion të rremë dhe të përgjojë të dhënat e transferuara ndërmjet tyre. Në shembullin e dytë, ndërhyrësi i paautorizuar po imiton të dyja anët e bisedës për të fituar akses në fonde, sulmuesi kap një çelës publik dhe me këtë mund të transpozojë kredencialet e tij për të mashtruar njerëzit në të dyja anët që ata të besojnë se po flasin me njëri-tjetrin në mënyrë të sigurt.

Helmimi i Kujtesës së DNS (DNS Cache Poisoning) është ndryshimi i cilësimeve lokale të DNS (duke ndryshuar vlerat reale të URL-ve), kështu që ju ose përdorni një server mashtrues DNS i cili ju drejton drejt kopjeve false të faqeve të Internetit, ose skedari lokal i hosteve në makina ndryshohet për të përmbajtur regjistrime të rreme. Helmimi i DNS bëhet gjithashtu për të injektuar programe keqdashëse në kompjuterin ose rrjetin tuaj. Pas vizitës te një faqe Interneti e rremë për shkak të kujtesës së helmuar të DNS, kriminelët mund të bëjnë gjithçka që duan. Kriminelët gjithashtu mund të konfigurojnë serverë të rremë DNS në mënyrë që kur këta të

marrin kërkesa, ata të mund të japin adresa IP të rreme. Ky helmim i DNS është i nivelit të lartë dhe korrupton shumicën e kujtesave të DNS në një zonë të caktuar duke prekur kështu shumë më tepër përdorues.

DNS Hijacking ose Ridrejtimi i DNS është një metodë e përdorur nga kriminelët kibernetikë për të rrëmbyer shfletuesin tuaj të internetit, ndërsa ai përpiqet të zgjidhë adresën IP të faqes së internetit që dëshironi të ngarkoni, përmes instalimit të programeve keqdashëse në kompjuterin tuaj për të ndryshuar DNS-në e paracaktuar si të besuar; kështu, sa herë që shfletuesi juaj përpiqet të zgjidhë një URL, për këtë ai kontakton një nga serverët e rremë DNS. Kjo bën që shfletuesi juaj të ngarkojë një faqe Interneti keqdashëse që mund të kompromet ojë kompjuterin tuaj ose të vjedhë kredencialet tuaja etj.

Në sulme të quajtura **Pharming** në një kompjuter personal ose server instalohet kod keqdashës, zakonisht si rezultat i ndërhyrjes në cilësimet e DNS, duke i keqdrejtuar përdoruesit drejt faqeve mashtruese të Internetit që janë kopje pothuajse identike e atyre reale, pa dijeninë apo pëlqimin e përdoruesve. Kjo është pjesë e procesit të phishing ku synohet mbledhja e informacionit personal nga viktimat.

Përshkallëzimi i privilegjeve (Privilege escalation) është shfrytëzimi i një gabimi, defekti në modelim apo vëmendjeje të paplotë në konfigurim në një sistem operativ ose program aplikativ për të fituar qasje më të lartë në burime që zakonisht nuk i lejohen një aplikacioni apo përdoruesi të zakonshëm. Si rezultat, një aplikacion me privilegje më të larta sesa është parashikuar nga zhvilluesi i aplikacionit ose administratori i sistemit mund të kryejë veprime të paautorizuara.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale që përfshijnë Mashtrimet

Infrastruktura Kritike Kombëtare

Infrastruktura Kritike Kombëtare (IKK) siguron shërbimet themelore që përbëjnë shtyllën mbajtëse të ekonomisë së kombit tonë, sigurisë, shëndetit, energjisë dhe ujit, transportit dhe sistemeve të komunikimit te të cilat mbështetemi çdo ditë, që janë aq jetike sa që rrëzimi ose shkatërrimi i tyre do të kishte një efekt rrënues në rendin publik, mirëqenien ekonomike, shëndetin publik, sigurinë kombëtare, apo një sërë prej tyre.

Sulmet kundër IKK mund të jenë të sponsorizuara nga shtetet e tjera, ideologjike, kriminale ose dashakeqëse. Më poshtë listohen shembuj të sulmeve të tilla.

Ndërhyrja e Paautorizuar në Infrastrukturë është një formë shkeljeje. Është përdorimi i paautorizuar apo qasja në kompjuterë ose burime të rrjetit

nëpërmjet shfrytëzimit të dobësive të identifikuara të sigurisë në rrjete. Ndërhyrja e paautorizuar mund të përdoret për të shpërfytyruar ose dëmtuar faqet e internetit (Shpërfytyrimi i faqeve në Internet dhe Dëmtimi i faqeve në Internet) dhe për të mbledhur të dhëna personale ose informacione të dobishme për kriminelët (Shkeljet e të dhënave).

Ndërhyrja e Paautorizuar në Pajisje është një sektor në rritje i krimit kibernetik, pasi rritja e Internetit të Gjërave (Internet of Things - IoT) i ka lidhur edhe më shumë pajisjet (përpos telefonave celularë dhe tabletave), por në shumë raste ato janë bërë më të cenueshme se kurrë më parë: ky lloj krimi sulmon që nga automobilat dhe pajisjet mjekësore deri te Infrastrukturat Kritike.

Haktivizmi (Hacktivism) është përdorimi i kompjuterëve dhe rrjeteve kompjuterike për të promovuar qëllime politike, pra kryerja e ndërhyrjeve të paautorizuara për një kauzë. Shumëkombëshet globale si kompanitë e naftës janë shpesh objektiva të haktivistëve.

Haktivitetet zakonisht përbëhen nga shpërfytyrimi i faqeve të internetit me deklarata politike ose realizimi i sulmeve të bllokimeve të shërbimit. Grupe të tilla si Lizard Squad, Mazafaka, OurMine, Anonymous dhe Lulzsec e kanë ngritur profilin e haktivizmit duke sulmuar faqet e mediave sociale apo shpërfytyruar faqet qeveritare të Internetit.

Relevanca Hetimet mbi Krimet Kompjuterike, Sulmet Kompjuterike

Ngacmimet

Bullizmi Kibernetik dhe Përndjekja Kibernetike mund t'u ndodhin *Viktimave Meshkuj* ose *Femra* dhe i referohen dikujt apo një grupi që përfshihet në sjellje sulmuese, kërcënuese apo ngacmuese ndaj të rinjve apo të rriturve. Sjellja mund të përfshijë mesazhe abuzive tekst ose e-mail, ose mesazhe, imazhe apo video lënduese.

Mobbing është njësoj si *Bullizmi Kibernetik dhe Përndjekja Kibernetike* por ka lidhje me vendin e punës.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale

Shërbime Kriminale me Pagesë!

Kriminelët përshtatin trajtime konvencionale që pasqyrojnë sjellje të ftohtë biznesi, që nga vendosja e çmimeve sipas stilit të supermarketeve, deri te kontraktimi i jashtëm, te specialistët që veprojnë si mushka, kodues, hakerë, shitës informacioni etj. Ka shumë më tepër role në nëntokën kriminale, që është një ekosistem i ndërlikuar ndërvarësish, me disa aftësi që vlerësohen mbi të tjerat. Më poshtë vijojnë shembuj të shërbimeve me pagesë:

Hakerët: Këta janë njerëzit që identifikojnë cenueshmërinë në programet komerciale. Aftësitë e tyre po rriten gjithnjë e më shumë ndërsa shohim përherë e më shumë gjetje të ditës (0day), emri ky që u jepet dobësive për të cilat kompanitë e programeve ose antiviruseve nuk janë në dijeni.

Koduesit: kanë aftësi të krijojnë programe për kompromentimin e të dhënave, për shembull.

Spamerët: Ata që kanë aftësi për të dërguar sasi të mëdha email-esh për qëllime të infektimit të makinave me programe keqdashëse, duke i drejtuar njerëzit në faqe për phishing ose duke u shitur atyre mallra të rreme (për shembull)

Shitësit: veprojnë kryesisht në forume – shesin të dhëna kartash krediti / për hyrje në sistemet bankare

Mushkat e Parave: personat që marrin të ardhurat nga mashtrimi me llogaritë bankare të kompromentuara dhe i kalojnë fondet në llogari që kontrollohen nga mashtruesit për t'u arkëtuar. Mund të jenë profesionistë ose të mashtruar për kryerjen e transaksioneve. Mbajnë një pjesë të parave.

Pastruesit e Parave: Shkëmbyes virtualë të parave që reklamojnë me vetëdije te kriminelët për shërbimin e transferimit të fitimeve virtuale të paligjshme në sistemin legjitim bankar / para të thata.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale që përfshijnë Mashtrimet

Shfrytëzimi Online i të Miturve

CCIU-ja ka ekipe të specializuara të trajnuara për të hetuar transferimet dhe shkëmbimet e imazheve që lidhen me shfrytëzimin seksual dhe abuzimin seksual të fëmijëve dhe për të hetuar grupet kriminale që përfitojnë nga publikimi ose shpërndarja e imazheve të abuzimit me fëmijët; mbështet policinë lokale me mjekësi ligjore kompjuterike dhe hetime të fshehta dhe siguron këshilla dhe mbështetje autoritative hetimore për të maksimizuar reagimin e policisë shqiptare ndaj krimeve të abuzimit dhe shfrytëzimit seksual të fëmijëve.

CCIU ndërlidhet me industrinë online dhe teknologjike për të minimizuar rrezikun e shfrytëzimit seksual dhe abuzimit seksual ndaj fëmijëve që vjen në sajë të teknologjisë së tanishme dhe të ardhshme.

Specialistët Policorë të Parandalimit punojnë së bashku me CCIU-në për të rritur njohuritë, aftësitë dhe mirëkuptimin e prindërve, kujdestarëve, fëmijëve dhe të rinjve.

Interneti përdoret për të transferuar dhe shkëmbyer *Abuzime të Fëmijëve me Imazhe të Pahijshme dhe gjithashtu për Transmetimin Drejtpërdrejt të Abuzimin me Fëmijët* ose *Shkarkimin e Materialeve të Abuzimit Seksual të Fëmijëve* ose bën të mundur përmbajtjes seksualisht fyese ose ekstreme për të rriturit (Transmetim i Drejtpërdrejtë ose i Shkarkueshëm), që është i paligjshëm sipas nenit 117/2 Pornografia e Fëmijëve.

Ekzaminimi i këtyre imazheve dhe informacioneve të lidhura me to mund të identifikojë se ku është abuzuar ose shfrytëzuar një fëmijë, dhe mund të çojë në largimin e fëmijës për te një vend të sigurt nga policia.

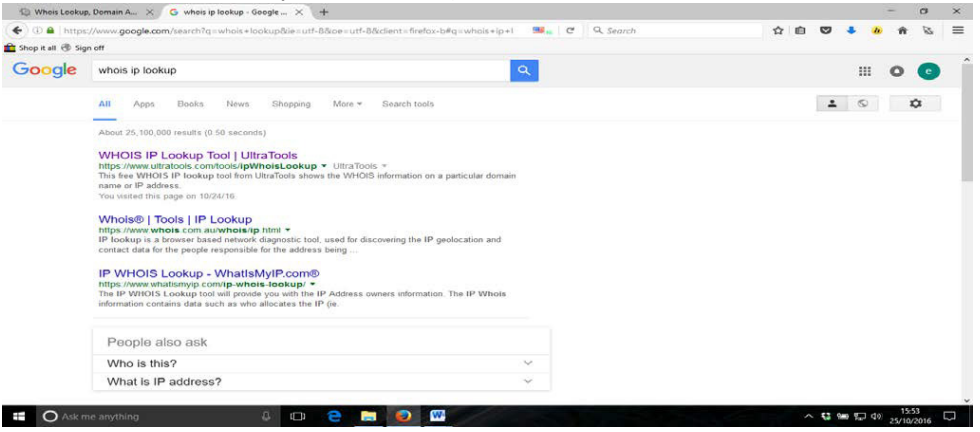
Hetimet e këtyre krimeve mund të jenë komplekse. Provat digjitale janë shpesh parësore dhe me rreziqe që lidhen me fëmijët. Është e domosdoshme që **në rast se identifikohen ose dyshohen krime të tilla, duhet të kontaktohet për mbështetje CCIU-ja.**

Shihni Udhëzime të Mëtejshme në shtojcën 'D'.

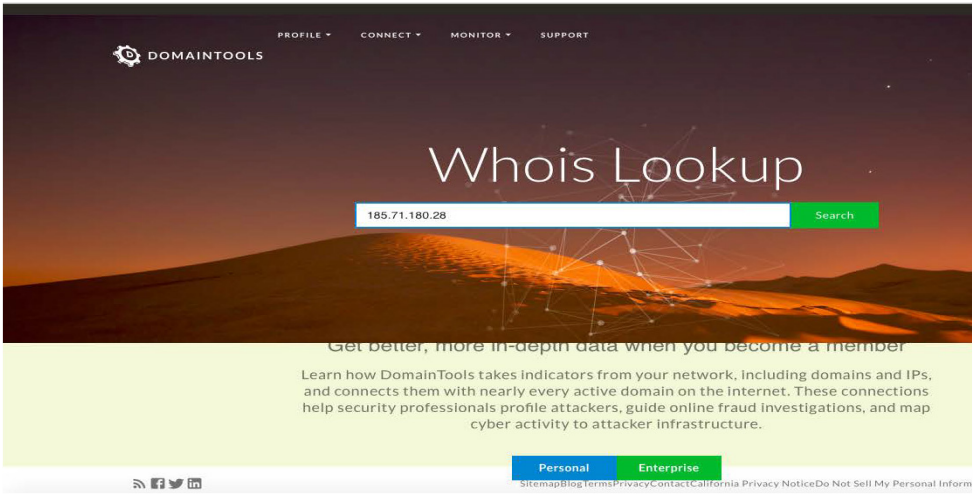
Relevanca: Hetimet mbi Shfrytëzimin e Fëmijëve, Hetimi i Krimeve Kompjuterike

Shtojca A – Udhëzime vizuale – Si të kërkoni një adresë IP ose subjektin regjistrues të një domeni

1. *Hapni një faqe për kërkime të IP me whois OSE (Hapni Google – shtypni "whois IP lookup" dhe kërkoni);*



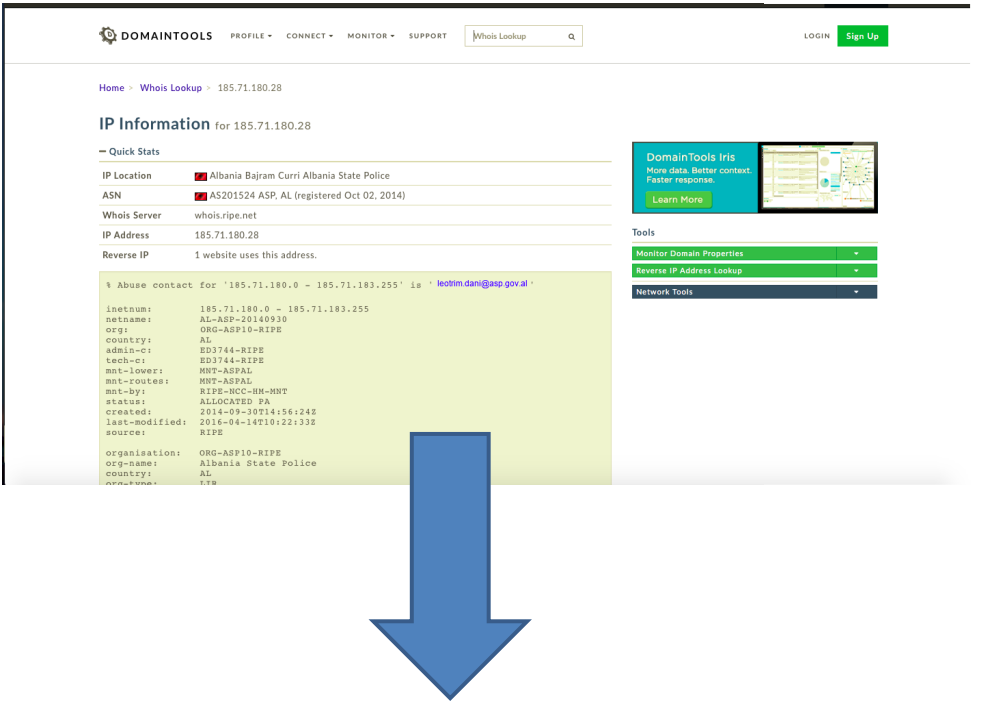
2. *Zgjidhni faqen– në këtë rast është http://whois.domaintools.com/ ;*



3. *Vendosni adresën IP, për shembull:* 185.71.180.28*, (ose, për domenin, emrin e faqes* **www.asp.gov.al***)*

4. *Shtypni* ⌦ *SEARCH;*

5. *Do të shfaqen rezultatet që vijojnë:*


DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home > Whois Lookup > 185.71.180.28
IP Information for 185.71.180.28
Quick Stats
IP Location
Albania Bajram Curri Albania State Police
ASN
AS201524 ASP, AL (registered Oct 02, 2014)
Whois Server
whois.ripe.net
IP Address
185.71.180.28
Reverse IP
1 website uses this address.
% Abuse contact for '185.71.180.0 - 185.71.183.255' is 'leotrim.dani@asp.gov.al'
inetnum: 185.71.180.0 - 185.71.183.255
netname: AL-ASP-20140930
org: ORG-ASP10-RIPE
country: AL
admin-c: ED3744-RIPE
tech-c: ED3744-RIPE
mnt-lower: MNT-ASPAL
mnt-routes: MNT-ASPAL
mnt-by: RIPE-NCC-HM-MNT
status: ALLOCATED PA
created: 2014-09-30T14:56:24Z
last-modified: 2016-04-14T10:22:33Z
source: RIPE
organisation: ORG-ASP10-RIPE
org-name: Albania State Police
country: AL
DomainTools Iris
More data. Better context. Faster response.
Learn More
Tools
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools

IP Information for 185.71.180.28

– Quick Stats

IP Location	Albania Bajram Curri Albania State Police
ASN	AS201524 ASP, AL (registered Oct 02, 2014)
Whois Server	whois.ripe.net
IP Address	185.71.180.28
Reverse IP	1 website uses this address.

```
% Abuse contact for '185.71.180.0 - 185.71.183.255' is ' emer.mbiemer@asp.gov.al

inetnum:        185.71.180.0 - 185.71.183.255
netname:        AL-ASP-20140930
org:            ORG-ASP10-RIPE
country:        AL
admin-c:        ED3744-RIPE
tech-c:         ED3744-RIPE
mnt-lower:      MNT-ASPAL
mnt-routes:     MNT-ASPAL
mnt-by:         RIPE-NCC-HM-MNT
status:         ALLOCATED PA
created:        2014-09-30T14:56:24Z
last-modified:  2016-04-14T10:22:33Z
source:         RIPE

organisation:   ORG-ASP10-RIPE
org-name:       Albania State Police
country:        AL
org-type:       LIR
address:        Bulevardi Bajram Curri
address:        1001
address:        Tirane
address:        ALBANIA
phone:          +355694118355
e-mail:         emer.mbiemer@asp.gov.al
abuse-c:        AC28059-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         MNT-ASPAL
mnt-ref:        MNT-ASPAL
mnt-by:         RIPE-NCC-HM-MNT
created:        2014-09-29T14:13:45Z
last-modified:  2021-02-03T09:27:27Z
source:         RIPE

person:         Edrin Dhroso
address:        Bulevardi Bajram Curri 1001 Tirane Albania
phone:          +355 694118663
e-mail:         emer.mbiemer@asp.gov.al
nic-hdl:        ED3744-RIPE
mnt-by:         MNT-ASPAL
created:        2014-09-30T08:08:22Z
last-modified:  2014-09-30T08:08:22Z
source:         RIPE

route:          185.71.180.0/24
descr:          Albania State Police
origin:         AS201524
mnt-by:         MNT-ASPAL
created:        2015-09-18T14:05:30Z
last-modified:  2015-09-18T14:05:30Z
```

Kjo është metodologjia me të cilën do të japin rezultate kërkimi shumica e mjeteve që janë falas. Ky proces kërkimi me mjetin online është i ngjashëm me kërkime të tjera të shtjelluara në **Mjetet e Kërkimit – Mjetet dhe bazat e të dhënave online për Analizimin e Adresave IP dhe Domeneve: Tipet e Kërkimeve**.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale, Bullizmi Kibernetik, Kërkimet për Adresat IP dhe të Domeneve

Shtojca B – Shpjegimi i regjistrimeve të të dhënave në Regjistrat Rajonalë të Internetit

Tabela që vijon është përkthim i rezultateve të mësipërme të kërkimit që u krye në ushtrimin për email në ***Shtojcën A***, dhe konverton të dhënat e koduara dhe termat teknikë në gjuhë të thjeshtë; ajo identifikon gjithashtu se çfarë përbën lidhje me hetimet penale rutinë dhe ato teknike me këto shënime:

- **RUTINË**: Ka lidhje me çdo hetim në lidhje me Internetin.
- **TEKNIK**: Lidhet me hetimet teknike për krimet kompjuterike – kërkoni mbështetje nga CCIU.
- **Bazë burimi të dhënash**: Informacion administrativ që lidhet me kërkesat e regjistrimit në bazën e të dhënave.

Të dhëna nga regjistri Whois	Të dhënat që mbahen në whois te www.domaintools.com	Shpjegimi i Terminologjisë	Hetimi
Informacion për adresën IP:	185.71.180.28	Adresa IP	RUTINË: Adresa IP subjekt i kërkimit ose hetimit.
Vendndodhja e IP:	 Albania Bajram Curri Albania State Police	Vendndodhja e adresës IP dhe emri i ISP të cilit i është alokuar ajo.	RUTINË: Ku është adresa IP? A përputhet vendndodhja me rrethanat e hetimit tuaj?
ASN	AS201524 ASP, AL (regjistruar më 02 tetor 2014)	Brenda Internetit, një Numër Sistemi Autonom (ASN) është një bashkësi prefiksesh për rutimet e IP që lidhen me njëra-tjetrën nën kontrollin e një apo më shumë operatorëve të rrjetit; ajo paraqet një politikë të përcaktuar për rutimet në Internet. Në këtë rast, ASN-ja është AS6821.	TEKNIK: Ky është numër unik dhe serveri përmban informacion rutimi dhe protokolle.

Whois Server	whois.ripe.net	Tregon që ky kërkim whois është kryer për serverin që administrohet nga Qendra Rajonale për Alokimin e Adresave IP, në këtë rast RIPE.	Bazë burimi të dhënash
Abuse contact for	Abuse contact for '185.71.180.0-185.71.183.255' is' emer.mbiemer@asp.gov.al	Adresa e email të kontaktit për çdo abuzim ose shkelje nga çdo adresë IP në këtë brez rrjeti.	KONTAKT TEKNIK
inetnum:	'185.71.180.0 - 185.71.183.255'	Tregon brezin e adresave IP që i janë alokuar kësaj ISP-je dhe vendosur nga RIPE si Regjistër Lokal Interneti (LIR).	RUTINË: A është adresa IP pjesë e këtij brezi.
netname:	AL-ASP-20140930	Emri i alokuar i rrjetit	TEKNIK: Emri i rrjetit
descr:	Albania State Police	Përshkrimi i Rrjetit – ADSL IP Subnet përcakton një Shërbim për Qasje në Internet	TEKNIK: Përshkrimi i veprimtarisë së rrjetit – Shërbim për ADSL IP subnet.
country:	AL	Vendi i Operatorit	RUTINË: shihni më sipër Vendndodhjen e IP.
admin-c:	ED3744-RIPE	Administratori përgjegjës	TEKNIK: Informacion
tech-c:	ED3744-RIPE	Tekniku përgjegjës	TEKNIK: Informacion
status:	ASSIGNED PA	LIR i alokuar dhe që lidhet me veprimet teknike operacionale	TEKNIK: Përshkrim i veprimtarisë së rrjetit
mnt-by:	MNT-ASPAL	Të dhëna administrimi	TEKNIK: Informacion
Created:	2015-09-18T14:05:30Z	Data e krijimit të regjistrimit	Bazë burimi të dhënash

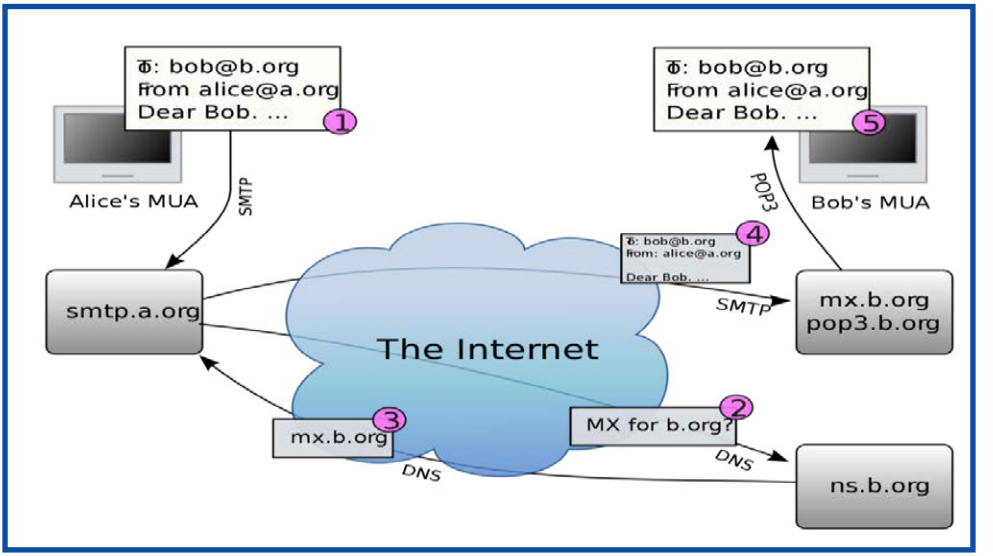
Last-modified:	2015-09-18T14:05:30Z	Data e freskimit të fundit	RUTINË: Bazë burimi të dhënash: kontrolloni datën për të parë se sa i freskët është informacioni.
source:	RIPE	Baza e të dhënave e RIPE	Bazë burimi të dhënash
role:	ADMIN	Administratori	RUTINË: Informacion mbi rolin ne ISP.
address:	Bulevardi Bajram Curri 1001 Tirane Albania phone: +355 694118663	Vendndodhja	RUTINË: Detaj i rëndësishëm kontakti për kërkime të dhënash dhe ndihmë teknike.
e-mail:	emer.mbiemer@asp.gov.al	Të dhënat e kontaktit, normalisht një adresë postare për Ekipin e Administrimit të Rrjetit	RUTINË: mund të mos plotësohet, pasi është vullnetare dhe shpesh është njësoj si adresa më lart për Abuzimet.
admin-c:	ED3744-RIPE	Administratori përgjegjës	TEKNIK: Informacion
tech-c:	ED3744-RIPE	Tekniku përgjegjës	TEKNIK: Informacion
nic-hdl:	MA12945-RIPE	Emri i Qendrës Informative të Rrjetit (NIC) është një varg karakteresh alfanumerike që përfaqëson një regjistrim në bazat e të dhënave që mirëmbahen nga Qendrat Informative të Rrjeteve. Sapo regjistrohet një domen, emri i tij si NIC mund të përdoret për të kërkuar atë regjistrim në bazën e të dhënave.	TEKNIK: Hetim – Identifikues i pajisjes

created:	2015-09-18T14:05:30Z	Data e krijimit të regjistrimit	Bazë burimi të dhënash
last-modified:	2015-09-18T14:05:30Z	Data e freskimit të fundit	Bazë burimi të dhënash
source:	RIPE	Baza e të dhënave e RIPE	Bazë burimi të dhënash
route:	185.71.180.0/24	Lidhet me politikën e rutimit; në këtë rast tregon adresimin e IP dhe protokollin e nënrrjetëzimit.	TEKNIK: Hetim për Rrjetin
descr:	Albania State Police	Emri i pajisjes që i jepet serverit.	TEKNIK: Hetim për Rrjetin
Origin:	AS201524	Secili AS (rrjet autonom) ka një numër unik (ASN), që shërben si identifikues në shkëmbimin e informacionit për rutimet e jashtme.	TEKNIK: Hetim për Rrjetin
mnt-by:	MNT-ASPAL	Të dhëna administruese për regjistrimin e ASN	TEKNIK: Hetim për Rrjetin
Created:	2015-09-18T14:05:30Z	Data e krijimit të regjistrimit	Bazë burimi të dhënash
last-modified:	2015-09-18T14:05:30Z	Data e freskimit të fundit	Bazë burimi të dhënash
source:	RIPE	Baza e të dhënave e RIPE	Bazë burimi të dhënash

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale, Bullizmi Kibernetik, Kërkimi për Adresat IP dhe Domenet

Shtojca C – Hetimi i Email

Kjo shtojcë ofron paraqitje vizuale dhe tekstuale të mënyrës se si funksionon emaili, protokollet e rrjetit për komunikim, ku ruhen të dhënat dhe çfarë informacioni ndodhet në titujt e postës elektronike që mund të ndihmojnë në hetimet penale. Procesi dhe protokollet e postës elektronike shpjegohen në fazat 1-5 në diagramin dhe **shpjegimin e mëposhtëm, për një email që dërgohet nga Alice te Bob.**



1. Alice@a.org shkruan një email te bob@b.org, mesazhi është krijuar në një kompjuter duke përdorur një program emaili: një klient email ose agjent përdoruesi të postës (*MUA*). Programi i postës elektronike kombinon tekstin që shkroi Alice (*trupi*) me detajet e marrësit bob@b.org, titullin e emailit, programi vendos një datë, orë, dhe zonën kohore në mesazh *(koka)*

2. Programi i postës elektronike (klienti/MUA) më pas dërgon mesazhin te një server i postës elektronike duke përdorur Protokollin e Thjeshtë të Transferimit të Mesazhit ose SMTP. Serveri i postës elektronike është një program që funksionon në një kompjuter tjetër që ndodhet në operatorin tuaj të shërbimit të internetit (ISP).

3. Në server, mesazhi zbërthehet dhe marrësit hiqen nga fushat To, Cc dhe Bcc në kokë. Serveri SMTP më pas gjen kompjuterin pritës për marrësit, serveri kërkon b.org dhe ia dërgon mesazhin atij kompjuteri. Për disa nanosekonda, mesazhi kalon nëpër internet ndërsa bën lidhjen me kompjuterin e destinacionit.

4. Në kompjuterin e destinacionit b.org, një server tjetër SMTP merr mesazhin dhe e vendos atë në një kuti postare të bob@b.org. Atje, ai pret derisa bob@b.org të hyjë për të mbledhur postën. Kutia postare në server nuk është e njëjta gjë si kutia postare në programin e postës së kompjuterit tuaj.

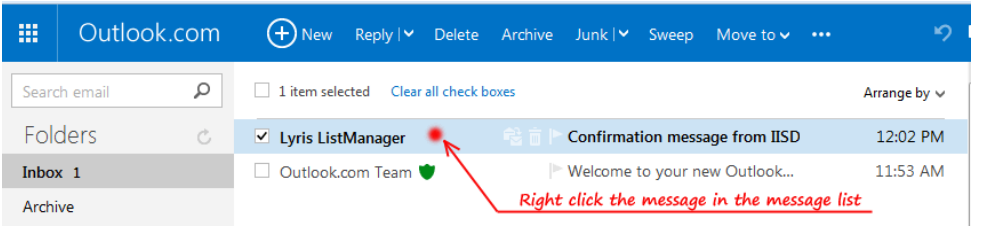
5. Bob hyn në programin e tij të postës dhe mbledh mesazhe të reja nga serveri i ISP-së së tij. Programi i postës përdor *Protokollin e Postës* (POP) për të marrë mesazhin. POP përdoret në vend të SMTP sepse mesazhi i emailit nuk po dërgohet më në internet; ka ardhur. Gjithçka që bën POP është marrja e mesazhit që po pret në server dhe transferimi i tij në kompjuterin e përdoruesit dhe në programin e tij të postës elektronike. Pasi mesazhet e postës janë në kompjuterin e marrësit, ato ruhen në një bazë të dhënash të organizuar nga programi i postës elektronike: p.sh. Inbox, Artikuj të Fshirë etj.

Metodat e postës elektronike të përshkruara këtu nuk zbatohen për sistemet e postës elektronike në organizata të mëdha, p.sh. Microsoft Outlook.

Përveç POP është metoda e *Protokollit të Qasjes së Mesazheve në Internet* (IMAP) për të lexuar emailin. Ndryshe nga POP, IMAP nuk i fshin mesazhet nga kutia postare e përdoruesit në server derisa përdoruesi të fshijë mesazhet. Programet e postës elektronike të bazuara në web, si Gmail dhe Hotmail, shpesh preferojnë IMAP. Këto informacione mund t'i zbulohen prokurorisë në mbështetje të një kërkese MLA.

Koka e plotë e emailit - si emailet e bazuara në web ashtu edhe ato të bazuara në klient, priren ta shkurtojnë kokën e emailit në Koha dhe data e marrjes, Nga, Titulli dhe trupi i emailit. Koka e plotë është ende aty, por duhet të hapet dhe email të ndryshëm të bazuar në web ofrojnë mënyra të ndryshme për të hyrë në kokën e plotë të emailit; p.sh. AOL kërkon që ju të qëndroni pezull mbi emailin e pahapur dhe të klikoni me butonin e djathtë të mausit dhe kjo do të zbulojë kokën dhe informacione të tjera burimore; Mail.com kërkon që emaili të hapet, më pas djathtas lart është një ikonë e shënuar 'i', kur klikohet kjo, shfaqet koka e plotë e emailit.

Nëse përballeni me një sistem emaili ku nuk e dini se ku do të jetë koka e zgjeruar, një kërkim në Google për *find extended email header in xxx*', shpesh jep një përgjigje siç tregohet me shembullin e mëposhtëm outlook.com



Çfarë po kërkojmë?

Analizimi i kokave shpesh nënkupton leximin e kokës së plotë nga fillimi deri në fund për të përcaktuar rastin e parë të secilit prej informacioneve më poshtë. Qëllimi i analizimit të kokës së mesazhit është të përpiqemi të identifikojmë adresën IP të dërguesit dhe të email-it të saktë origjinal prej nga është dërguar mesazhi. Informacionet nga koka janë më të sakta dhe relevante dhe këto informacione mund të përdoren si prova.

- Informacioni i dërguesit
- Adresa IP origjinuese me kohën origjinale të mbërritjes
- Dërguesi i parë me një adresë të jashtme për ISP-në
- Dërguesi i parë me një adresë të brendshme
- Kokat e Zgjeruara/Plota

Informacione të tjera që mund të ndihmojnë në identifikimin e pajisjes së përdorur përfshijnë:

- Përshkrimi i programit të email
- Gjuha e programit
- Informacion lokal për pajisjen
- Informacion lokal për emailin

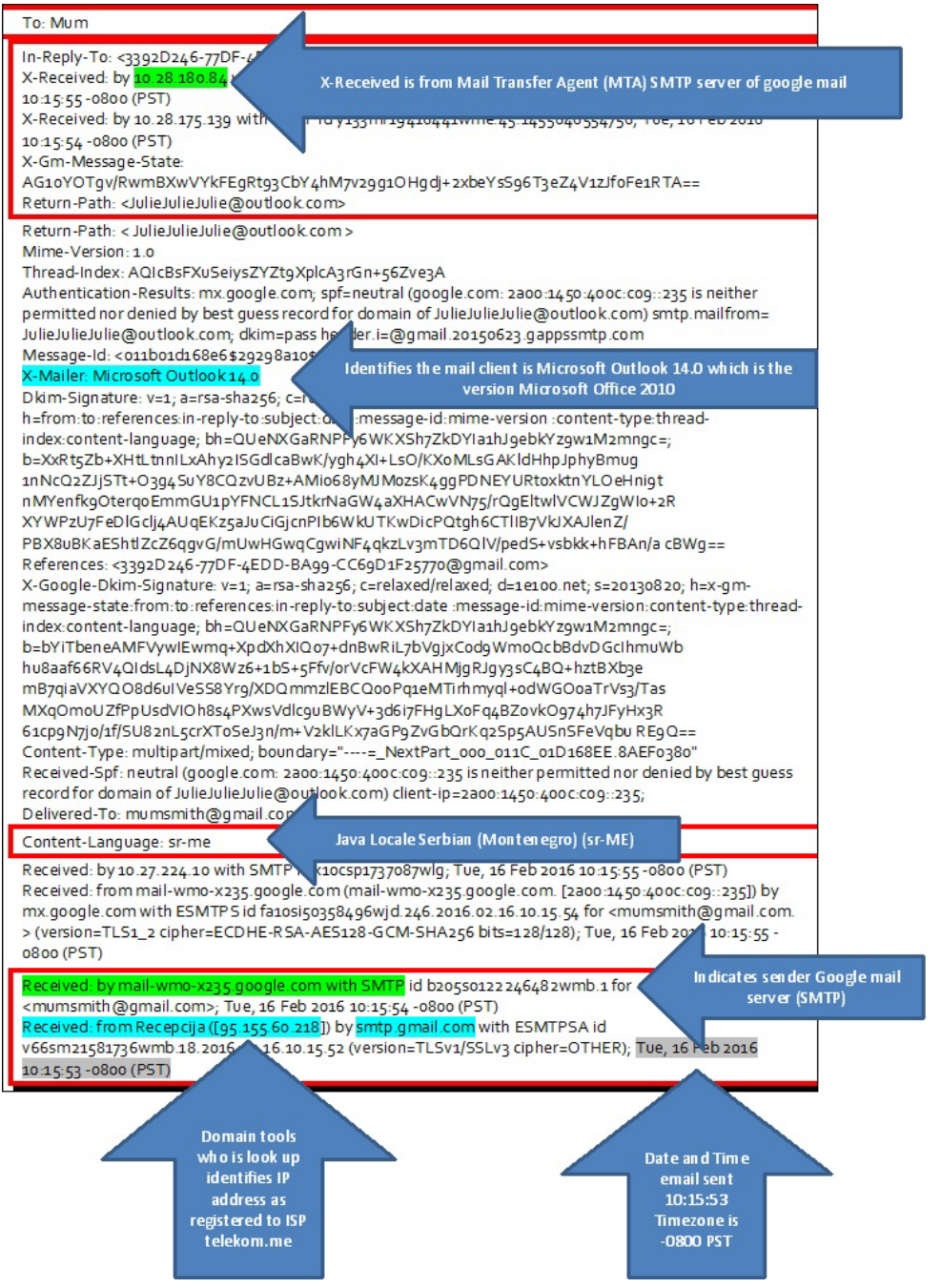
Për shkak të rasteve së fundmi që lidhen me privatësinë, disa kompani i fshijnë këto detaje nga emaili ose i shifrojnë ato, kështu që ato bëhen të palexueshme.

Relevanca: Hetimet mbi Krimet Kompjuterike, Hetimet Penale, Bullizmi Kibernetik, Kërkimi për Adresat IP, Hetimi i Email

Shembull i një koke të plotë email-i

To: Mum
In-Reply-To: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
X-Received: by 10.28.180.84 with SMTP id d81mr21959784wmf.42.1455646555118; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
X-Received: by 10.28.175.139 with SMTP id y133mr19416441wme.45.1455646554756; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
X-Gm-Message-State:
AG10YOTgv/RwmBXwVYkFEgRt93CbY4hM7v29g1OHgdj+2xbeYsS96T3eZ4V1zJfoFe1RTA==
Return-Path: <JulieJulieJulie@outlook.com>
Return-Path: < JulieJulieJulie@outlook.com >
Mime-Version: 1.0
Thread-Index: AQIcBsFXuSeiysZYZt9XplcA3rGn+56Zve3A
Authentication-Results: mx.google.com; spf=neutral (google.com: 2a00:1450:400c:c09::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) smtp.mailfrom=JulieJulieJulie@outlook.com; dkim=pass header.i=@gmail.20150623.gappssmtp.com
Message-Id: <011b01d168e6$29298a10$7b7c9e30$@gmail>
X-Mailer: Microsoft Outlook 14.0
Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.20150623.gappssmtp.com; s=20150623; h=from:to:references:in-reply-to:subject:date:message-id:mime-version:content-type:thread-index:content-language; bh=QUeNXGaRNPFy6WKXSh7ZkDYIa1hJ9ebkYz9w1M2mngc=; b=XxRt5Zb+XHtLtnnILxAhy2ISGdlcaBwK/ygh4XI+LsO/KXoMLsGAKldHhpJphyBmug
1nNcQ2ZJjSTt+O3g45uY8CQzvUBz+AMio68yMJMozsK4ggPDNEYURtoxktnYLOeHni9t
nMYenfk9OterqoEmmGU1pYFNCL1SJtkrNaGW4aXHACwVN75/rQgEltwlVCWJZgWIo+2R
XYWPzU7FeDlGclj4AUqEKz5aJuCiGjcnPIb6WkUTKwDicPQtgh6CTIIB7VkJXAJlenZ/
PBX8uBKaEShtlZcZ6qgvG/mUwHGwqCgwiNF4qkzLv3mTD6QlV/pedS+vsbkk+hFBAn/a cBWg==
References: <3392D246-77DF-4EDD-BA99-CC69D1F25770@gmail.com>
X-Google-Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20130820; h=x-gm-message-state:from:to:references:in-reply-to:subject:date :message-id:mime-version:content-type:thread-index:content-language; bh=QUeNXGaRNPFy6WKXSh7ZkDYIa1hJ9ebkYz9w1M2mngc=; b=bYiTbeneAMFVywIEwmq+XpdXhXIQo7+dnBwRiL7bVgjxCod9WmoQcbBdvDGcIhmuWb
hu8aaf66RV4QIdsL4DjNX8Wz6+1bS+5Ffv/orVcFW4kXAHMjgRJgy3sC4BQ+hztBXb3e
mB7qiaVXYQO8d6uIVeSS8Yr9/XDQmmzlEBCQooPq1eMTirhmyql+odWGOoaTrVs3/Tas
MXqOmoUZfPpUsdVIOh8s4PXwsVdlc9uBWyV+3d6i7FHgLXoFq4BZovkO974h7JFyHx3R
61cp9N7jo/1f/SU82nL5crXToSeJ3n/m+V2klLKx7aGP9ZvGbQrKq2Sp5AUSnSFeVqbu RE9Q==
Content-Type: multipart/mixed; boundary="----=_NextPart_000_011C_01D168EE.8AEF0380"
Received-Spf: neutral (google.com: 2a00:1450:400c:c09::235 is neither permitted nor denied by best guess record for domain of JulieJulieJulie@outlook.com) client-ip=2a00:1450:400c:c09::235;
Delivered-To: mumsmith@gmail.com
Content-Language: sr-me
Received: by 10.27.224.10 with SMTP id x10csp1737087wlg; Tue, 16 Feb 2016 10:15:55 -0800 (PST)
Received: from mail-wm0-x235.google.com (mail-wm0-x235.google.com. [2a00:1450:400c:c09::235]) by mx.google.com with ESMTPS id fa10si50358496wjd.246.2016.02.16.10.15.54 for <mumsmith@gmail.com. > (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128); Tue, 16 Feb 2016 10:15:55 -0800 (PST)
Received: by mail-wm0-x235.google.com with SMTP id b205s012224682wmb.1 for <mumsmith@gmail.com>; Tue, 16 Feb 2016 10:15:54 -0800 (PST)
Received: from Recepcija ([95.155.60.218]) by smtp.gmail.com with ESMTPSA id v66sm21581736wmb.18.2016.02.16.10.15.52 (version=TLSv1/SSLv3 cipher=OTHER); Tue, 16 Feb 2016 10:15:53 -0800 (PST)
RE: Where are you?

Informacioni në email që lidhet me një hetim:



Shtojca D – Udhëzime për realizimin e hetimeve fillestare mbi krimet kompjuterike dhe trajtimi i të dhënave digjitale.

Shtojca D synon të formojë bazën e një manuali për hetimin e çështjeve të krimeve kompjuterike kur merren raportet fillestare të krimeve kompjuterike ose krimeve të lidhura me kompjuterat dhe gjatë vizitës fillestare te vendi i krimit.

Ajo synon gjithashtu t'u mundësojë hetuesve që të jenë në gjendje të bëjnë hetime paraprake mbi adresat e emailit, adresat IP, si dhe vendndodhjet dhe regjistrimet e faqeve në Internet, pasi provat digjitale kryqëzohen me të gjitha format e krimit.

Secili prej udhëzimeve trajton një fushë specifike:

1. Ankesa e qytetarëve për krime kompjuterike ose krime që lidhen me kompjuterat;
2. Marrja e provave nga një biznes i prekur nga krimi kompjuterik - Rrjetet e Mediave Digjitale, kompjuterët, laptopët, pajisjet për ruajtjen e të dhënave/ mediave dhe pajisjet celulare;
3. Hetimi i krimeve që përfshijnë media digjitale - kompjuterë, laptopë dhe pajisje për ruajtjen e të dhënave/mediave;
4. Hetimi i krimeve që përfshijnë media digjitale - telefonat inteligjentë dhe pajisje të tjera celulare;
5. Menaxhimi dhe sekuestrimi i provave hetimore në lidhje me Imazhet e Abuzimit të Fëmijëve (Pornografia e Fëmijëve) të ruajtura në Media Digjitale;
6. Përftimi i të dhënave nga operatorët kombëtarë dhe ndërkombëtarë të shërbimeve të Internetit.

Raportimi i qytetarëve për krim kompjuterik ose krim të lidhur me kompjuterët

Raportimi i qytetarëve për krim kompjuterik ose krim të lidhur me kompjuterët.

Ky udhëzues shërben për të mbështetur një prokuror dhe efektiv policie që merr nga një qytetar ose biznes të vogël një ankesë fillestare për krim që përfshin prova digjitale dhe si të ruajë dhe marrë në mënyrë të sigurtë dhe të ligjshme prova nga një pajisje digjitale e viktimave si telefoni, kompjuteri ose pajisje e ruajtjes së të dhënave/mediave. (Për informacion shtesë mbi organizatat dhe bizneset që kanë rrjete dhe serverë të mëdhenj, shihni ankesën e Biznesit ose Organizatës së Madhe për krimin kompjuterik).

Provë digjitale është çdo informacion ose e dhënë me vlerë për një hetim, e cila ruhet, merret ose transmetohet nga një pajisje elektronike. Mesazhet me tekst, SMS, kontaktet, thirrjet drejt dhe nga një pajisje, emailet, fotografitë, videot, skedarët dhe kërkimet në internet janë disa nga llojet më të zakonshme të provave digjitale.

Ndërveprimi i një të dyshuari me një pajisje tjetër elektronike gjatë kryerjes së krimeve kompjuterike ose krimeve të aktivizuara me kompjuter do të lërë një gjurmë mjekoligjore digjitale.

Provat Digjitale/Veprimet e Prokurorisë	Procesi hetimor
Çështja i raportohet prokurorisë: *Prokuroria:* Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar.	• Qëllimi kriminal; • Vendndodhja dhe koha e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; • Provat e krimit
Raporti me informacion rreth çështjes i dorëzohet prokurorisë. Prokuroria: - ***Identifikon veprën penale që duhet të hetohet.*** - ***Identifikon nëse provat mund të merren në format elektronik ose në letër*** - ***Identifikon autoritetin ligjor që mban provat, Përgatit Urdhrin për ruajtjen dhe zbulimin e të dhënave*** - ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimin kriminalistik të pajisjeve.*** ***Shtesë:*** ***Prokuroria mund të kërkojë mbledhjen dhe regjistrimin e të dhënave nga Burime të Hapura (OSINT)***	1. Identifikoni shkeljen dhe çështjet për të provuar; 2. Identifikoni provat e nevojshme për të vërtetuar veprën penale; 3. Identifikoni autoritetin ligjor për sekuestrimin e provave; 4. Identifikoni nëse provat nga viktima mund të sigurohen në mënyrë elektronike ose në printime në letër; 5. Evidentoni sekuestrimin e dokumenteve apo provave elektronike; **OSE** 6. A ka nevojë pajisja të imazhohet dhe të ekzaminohet? 7. Merrni autorizim me shkrim nga viktima për të ekzaminuar pajisjen. 8. Të merreni me sekuestrimin dhe ruajtjen e provave në një pajisje digjitale? – Shkoni te **Statusi i Pajisjes**:

E rëndësishme:
Ruajtja dhe mbledhja e saktë e provave, përfshirë provat digjitale, është e rëndësishme.

A po ndodh krimi tani apo ka ndodhur tashmë? A ka këtu ndonjë element që është kritik për kohën, p.sh. të dhënat po fshihen nga distanca, kërcënim për jetën?

Statusi i Pajisjes:

A është Pajisja Elektronike/Digjitale e Ndezur apo e Fikur?

Pajisja është e Ndezur – Shkoni te 10.
Pajisja është e Fikur – Shkoni te 18.

Pajisja është e Ndezur:

Prokuroria:

Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.

Prokuroria mund të kërkojë sekuestrimin e të dhënave kompjuterike nëse kompjuteri është i ndezur dhe ka rrezik për humbjen e të dhënave pas fikjes.

Prokuroria duhet të këshillojë grupin hetimor që të dokumentojë çdo veprim në skenë gjatë kërkimit dhe sekuestrimit

MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT

Ruajtja dhe mbledhja e saktë e provave, përfshirë provat digjitale, është

E Rëndësishme.

A janë shfaqur prova në pajisje?

Nëse krimi përfshin dikë që komunikon me një tjetër, p.sh. mashtrim, kërcënim, programe shpërblese, policia gjyqësore duhet të sigurojë që ato nuk po komunikojnë më tej pa e konsultuar çështjen së pari me prokurorinë.

Çfarë do të humbasë po të shkëputet rrjeti?

Çfarë pasoje do të ketë në hetimin tuaj përdorimi i pajisjes për të marrë prova?

Po fshihen ose korruptohen të dhëna nga Programe Keqdashëse?

MOS E FIKNI PAJISJEN – Kjo do të ndryshojë provat.

9. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi;
10. Nëse provat shfaqen dukshëm në ekran, shkrepni fotografi dhe mbani shënime për çdo material në ekranin e kompjuterit dhe programet e shfaqura në task bar;

Vetëm inspektim vizual

Mos u tundoni të lëvizni në kompjuter duke përdorur mausin ose tastierën.

11. Kërkoni të gjithë karikuesit ose manualet për pajisjen;
12. Pyetni Viktimën për fjalëkalimin dhe/ose numrin PIN të pajisjes dhe veçori të tjera sigurie si ato biometrike apo, në rastin e shifrimit, pyetni viktimën për fjalëkalimin/frazëkalimin dhe mbani regjistrim të detajeve.
13. Për të Shmangur Ndryshime në Largësi të të Dhënave – konsideroni izolimin e pajisjes nga Ethernet, Wi-Fi apo rrjeti i komunikimit. Me një pajisje celulare apo laptop, nëse jeni kompetent, konsideroni ndryshimin në "airplane mode" dhe regjistroni veprimet;
14. Nuk jeni të sigurt për mbylljen e pajisjes apo shkëputjen e rrymës?

Nëse nuk jeni të sigurt apo kompetentë për të kryer veprimet në pikën 12 ose 13, kërkoni ndihmë nga një teknik me përvojë – CCIU/DFU.

	15. Nëse ka tregues që kompjuteri ka të instaluara programe keqdashëse të cilat po fshijnë apo korruptojnë të dhëna nga hard disku, shkëputeni pajisjen menjëherë nga burimi i rrymës, në rastin e një laptopi ose celulari hiqni edhe baterinë. Regjistroni arsyen dhe veprimet që keni marrë. 16. Shkoni te **Sekuestrimi i Pajisjes**.
Pajisja e Fikur? ***Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.*** ***Prokuroria duhet të këshillojë grupin hetimor që të dokumentojë çdo veprim në skenë gjatë kërkimit dhe sekuestrimit*** ***Këshilloni hetuesin që të marrë të gjitha kredencialet për pajisjet e sekuestruara***	**MOS E NDIZNI** kjo do të ndryshojë provat. 17. Pyetni viktimën për fjalëkalimet, përcaktoni nëse pajisja është e kriptuar, pyetni viktimën për fjalëkalimin/ frazëkalimin; 18. Siguroni karikuesin dhe manualet e pajisjes. **MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT** 19. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi. 20. Shkoni te **Sekuestrimi i Pajisjes**.
Pajisjet e Ruajtjes së të Dhënave dhe Mediave: ***Shembuj të këtyre pajisjeve përfshijnë, Hard Disqet (USB/Wireless) USB Memory sticks, DVD, karta SD etc.*** ***Prokuroria duhet të këshillojë grupin hetimor që të dokumentojë çdo veprim në skenë gjatë kërkimit dhe sekuestrimit***	21. Nëse pajisja është **'e ndezur'** ose e lidhur me një kompjuter në linjë që është 'i ndezur' atëherë çdo shkëputje mund të shkaktojë ndryshime në të dhëna dhe ose të shkaktojë humbjen e të dhënave. Trajtojeni pajisjen si në Veprimin 12-14. 22. Nëse pajisja është e izoluar dhe/ose e fikur Veprimi si në 16-18. 23. Shkoni te **Sekuestrimi i Pajisjes.**
Të Dhënat e Komunikimit të Telefonave Inteligjentë ose Pajisjeve të Lëvizshme: ***(IMEI - Identiteti Ndërkombëtar i Pajisjeve Celulare)*** ***IMSI - Identiteti Ndërkombëtar i pajtimtarit celular)*** ***Prokuroria po lëshon Urdhër për zbulimin e komunikimit telefonik nga operatori telefonik kombëtar për numrin e identifikuar të telefonit dhe më shumë informacion për numrin IMEI***	24. Siguroni nga viktima identifikuesit e pajisjes: • Numrin e telefonit • numrin IMEI • numrin IMSI; 25. Miratim me shkrim nga viktima për të siguruar të dhënat e komunikimit nga CSP Operatori i Shërbimeve të Komunikimit dhe/ose Operatori i Shërbimeve të Internetit.

Operatorët e Rrjeteve Sociale /Ankandeve/ Shitblerjeve/ Email Providers: ***Provat e postës elektronike dhe të mediave sociale me pëlqimin e viktimës mund të merren nga kutia postare ose llogaria e viktimës.*** ***Të dhënat e trafikut dhe regjistrimet në lidhje me email etj. të mbajtura nga CSP ose Faqja e Rrjetit Social (SNW) mund të merren vetëm nga Prokuroria /Gjykata.*** ***Shumica e CSP dhe SNW kanë në faqet e tyre udhëzues për agjencitë e zbatimit të ligjit se çfarë të dhënash mbahen dhe për sa kohë.*** ***Prokuroria duhet të lëshojë urdhër për ruajtjen e të dhënave nëse të dhënat po mbahen nga një operator ndërkombëtar i shërbimeve të Internetit.*** ***Prokuroria duhet të lëshojë një urdhër për zbulimin e të dhënave nëse të dhënat po mbahen nga një operator kombëtar i shërbimeve të Internetit***	26. A zotëron llogaria e viktimave prova digjitale të krimit tashmë? **Po** – përcaktoni se si mund t'i shkarkoni si prova me miratimin e viktimave. Merrni në konsideratë metodën më të mirë për marrjen e skedarëve/videove provë? 27. Përcaktoni nëse viktima mund të sigurojë të dhënat për provë si pjesë e termave dhe kushteve. 28. Faqet e Rrjeteve Sociale/Ankandeve/ Shitblerjeve – Merrni nga viktima Emrin e Përdoruesit, emrin e Llogarisë dhe numrin identifikues unik të Llogarisë së tyre; 29. Llogaritë e Email - Merrni nga viktima emrin e llogarisë dhe adresat e email; 30. Identifikoni datat që lidhen me shkeljet penale; 31. Merrni nga viktima miratim me shkrim për të marrë të dhëna nga këta operatorë shërbimesh;
Sekuestrimi i Pajisjes: ***PARALAJMËRIM – Mund të jetë nevoja të mblidhni prova forensike të tjera përfshirë gjurma gishtash, mostra biologjike, ADN, etc. nga pajisjet. Këshillohuni me efektivët forensikë të skenave të krimit për të ruajtur provat dhe integritetin e të dhënave në pajisje.*** ***Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara.***	32. Informoni viktimën pse po sekuestrohet pajisja dhe për sa kohë; 33. Merrni miratim me shkrim nga viktima për ekzaminim mjekoligjor të pajisjes; 34. Sekuestroni dhe Paketoni pajisjen sipas PSO/Ligjit; 35. Merrni në konsideratë që të kërkoni kompjutera të tjerë ose pajisje të tjera për ruajtje të dhënash që mund të përmbajnë kopje (backup) të pajisjes; 36. Paketojeni pajisjen në mënyrë që të mos dëmtohet fizikisht apo të deformohet; 37. Paketojeni pajisjen në qese apo kuti provash; 38. Materialet e rrezikshme në pajisje duhet të detajohen në paketim dhe të informohet DFU.

Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Ky proces duhet të jetë i shpejtë me qëllim që të mos humbasin prova***	39. Dorëzojini provat te një objekt i sigurt i zbatimit të ligjit ose laborator provash digjitale sa më shpejt të jetë e mundur; 40. Mbroni nga temperaturat ekstreme, elektriciteti statik, fushat magnetike apo lagështia. 41. Mbani regjistrim Auditimi për vazhdimësinë e provave.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Urdhri nga prokuroria duhet të konkretizojë se për çfarë provash duhet të kryhet kërkimi.*** ***Urdhri duhet të ketë përshkrimin dhe numri serial të saktë të secilës prej provave materiale***	42. Informojeni prokurorinë për shkeljet Penale të identifikuara dhe Procedurat e Ndërmarra. 43. Merrni Autorizim/Urdhër nga prokuroria për hetim të mëtejshëm.
Prokuroria mund të ndjekë procesin e kriminalistikës digjitale dhe nxjerrjes së provave digjitale	**Nëse pajisjet janë sekuestruar për Imazhim ose Ekzaminim Digjital Mjekoligjor; informoni DFU për materialet e sekuestruara dhe vendimet hetimore të prokurorisë.**

Marrja e provave nga një Biznes të prekur nga krimi kompjuterik - Rrjetet e Mediave Digjitale, Kompjuterat, Laptopët, Pajisjet e ruajtjes së të Dhënave/Mediave dhe Pajisjet e Lëvizshme

Ankesa e një biznesi ose organizate të madhe për krim kompjuterik ose krim të lidhur me kompjuterat
Rrjetet e Mediave Digjitale, Kompjuterat, Të Dhënat, Pajisjet e Lëvizshme dhe Sulmet me Programe Keqdashëse

Bizneset dhe organizatat e mëdha publike ose private ka të ngjarë të përballen me krime kompjuterike njësoj si qytetarët, por gjithashtu do të jenë të prekshëm nga sulmet e ndërhyrësve të paautorizuar dhe programet keqdashëse. Disa prej këtyre sulmeve kryhen ndaj bizneseve dhe organizatave që janë pjesë e Infrastrukturës Kritike Kombëtare të Shqipërisë; të tjerët do të përballen me ndikim financiar nga sulmet dhe mund të ngurrojnë të raportojnë krimin. Në këto raste është e rëndësishme për prokurorinë që CCIU të informohet për krimin sa më parë.

Bizneset dhe organizatat e mëdha shpesh duhet të trajtohen ndryshe kur janë viktima të krimit kompjuterik ose krimit të lidhur me kompjuterat, mund të jetë e dëmshme për punën e tyre heqja e pajisjeve nga vendi i punës, dhe do të jetë e dëmshme nga ana tregtare shkëputja e biznesit nga rrjetet ose Interneti me qëllim të marrjes së provave.

Në shumicën e rasteve do të jetë e nevojshme të identifikoni individët kryesorë përgjegjës për biznesin (CEO) dhe rrjetet dhe infrastrukturën digjitale, përgjegjës për trajtimin e një 'incidenti kibernetik' (menaxher / inxhinier / administrator i rrjetit, i kontraktuar ose i brendshëm) dhe të këshilloheni me ta në një fazë të hershme së bashku me CCIU/DFU dhe prokurorinë.

Gjatë një incidenti kibernetik, një organizatë viktimë duhet të bëjë menjëherë një vlerësim të natyrës dhe fushës së incidentit për të përcaktuar nëse incidenti është një veprim keqdashës apo një defekt teknologjik.

Telefonat inteligjentë, mediat digjitale, kompjuterat, serverat, ruterët dhe pajisjet e ruajtjes së të dhënave do të përmbajnë prova digjitale. Provë digjitale është çdo informacion ose e dhënë me vlerë për një hetim që ruhet, merret ose transmetohet nga një pajisje elektronike.

Ndërveprimi i një të dyshuari me një pajisje tjetër elektronike gjatë kryerjes së krimeve kompjuterike ose krimeve të aktivizuara me kompjuter do të lërë një gjurmë mjekoligjore digjitale.

Provat Digjitale/Veprimet e Prokurorisë	Procesi hetimor
Çështja i raportohet prokurorisë: ***Prokuroria:*** Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar. ***Pajisjet dhe rrjetet e kompanisë mund të përmbajnë informacion kritik për të provuar një vepër penale***	• **Identifikoni** - Qëllimin kriminal; • Vendndodhja dhe koha e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; • Provat e krimit.

Prokuroria: - ***Identifikon veprën penale që duhet të hetohet.*** - ***Identifikon nëse provat mund të merren në format elektronik ose në letër*** - ***Identifikon autoritetin ligjor që mban provat, Përgatit Urdhrin për ruajtjen dhe zbulimin e të dhënave*** - ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimin kriminalistik të pajisjeve.*** - ***Identifikon se cilin profil eksperti të përfshijë në procesin e identifikimit dhe sekuestrimit të provave elektronike*** - ***Prokuroria duhet të japë urdhër për sekuestrimin e të dhënave kompjuterike, kryerjen e kriminalistikës në kohë reale ose sekuestrimin e tërë pajisjeve që kanë prova elektronike*** ***Identifikoni personat kyç nga Organizata*** ***Është e rëndësishme të arrihet që provat, përfshirë edhe provat digjitale, të Ruhen dhe të Mblidhen.***	1. Identifikoni shkeljen; 2. Identifikoni personin përgjegjës/marrësit e vendimeve, përgjegjës për çdo veprim që mund të ndikojë drejtpërdrejt në punë : • Biznesi (CEO/Administratori/Pronari) • Rrjeti dhe Infrastruktura (Menaxheri, Inxhinieri, Administratori i Rrjetit); • Menaxhimi i një Incidenti Kibernetik. • Palë të treta operatore të shërbimeve të përfshira nga kompania për të siguruar elementë të infrastrukturës së rrjetit dhe biznesit që po sulmohet (ISP-të, CSP-të, programe ose ruajtje të dhënash në Largësi apo në Cloud etj.); 3. Identifikoni ku janë provat; 4. Identifikoni autoritetin ligjor për sekuestrimin/ ekzaminimin e provave; 5. Siguroni skenën; 6. Identifikoni nëse provat e viktimës duhet dhënë: • Elektronikisht; • Të printuara; 7. Ka nevojë që pajisja të sekuestrohet, imazhohet dhe/ose ekzaminohet në vend apo mund të nxirret jashtë? • Imazh Forensik (DFU); • Imazhim Forensik i Drejtpërdrejtë (DFU); • Forensika e Drejtpërdrejtë (DFU). 8. Evidentoni sekuestrimin e dokumenteve apo provave elektronike sipas PSO; **OSE** 9. Merrni autorizim me shkrim nga viktima për të sekuestruar dhe ekzaminuar pajisjen. 10. Të merreni me sekuestrimin dhe ruajtjen e provave në një pajisje digjitale? – Shkoni te **Statusi i Pajisjes:**
Prokuroria/Hetuesia ndjek veprimet e ndërmarra nga Menaxheri / Inxhinieri / Administratori i Rrjetit: ***ASNJË veprim nuk duhet të shkatërrojë prova elektronike***	11. Përcaktoni nëse biznesi ka një plan reagimi ndaj incidenteve kibernetike. 12. Kërkoni që ata të mbajnë një procesverbal të vazhdueshëm dhe me shkrim të të gjithë hapave të ndërmarrë, aty ku është e mundur. 13. A janë aktivizuar aftësitë e duhura të regjistrimit të rrjetit pasi këto mund të jenë kritike për identifikimin e shkakut të incidentit kibernetik?

Nëse është nevoja, prokuroria lëshon një urdhër për sekuestrimin e disa të dhënave kompjuterike për analizim (zakonisht regjistrime nga serverët)

Ruajtja dhe mbledhja e të dhënave përfshirë të dhënat digjitale është e rëndësishme

Izolimi i çdo sulmi kibernetik është prioritet pune!

Prokuroria duhet të këshillojë grupin hetimor që të dokumentojë çdo veprim në skenë gjatë kërkimit dhe sekuestrimit

14. Në rast të një sulmi të vazhdueshëm, kërkoni që të merret parasysh rritja e madhësisë së paracaktuar të skedarëve të regjistrimeve në serverët e tij për të parandaluar humbjen e të dhënave.
15. Kërkoni ruajtjen e regjistrave përkatës ekzistues.
16. Duke përdorur informacionin e regjistrimeve, një administrator i sistemit duhet të përpiqet të identifikojë:
    - Sistemet kompjuterike të prekura;
    - Origjinën në dukje të incidentit, ndërhyrjes ose sulmit;
    - Çdo program keqdashës të përdorur në lidhje me incidentin;
    - Çdo server në distancë tek i cili dërgoheshin/po dërgoheshin të dhëna të paautorizuara;
    - Identitetin e çdo organizate tjetër viktimë, nëse të dhëna të tilla janë të dukshme në të dhënat e regjistruara.
17. Përcaktoni dhe dokumentoni:
    - Cilët përdorues kanë hyrë aktualisht në sistem;
    - Cilat janë lidhjet aktuale me sistemet kompjuterike;
    - Cilat procese po ekzekutohen;
    - Të gjitha portet e hapura, shërbimet dhe aplikacionet e lidhura me to.
18. Çdo komunikim (në veçanti, kërcënimet ose kërkesat për zhvatje) i marrë nga organizata që mund të lidhet me incidentin duhet t'i jepet policisë **dhe** gjithashtu të ruhet;
19. Thirrjet e dyshimta, emailet ose kërkesat e tjera për informacion duhet të trajtohen si pjesë e incidentit dhe të ruhen si provë;
20. Dokumentoni dhe ruani provat se ka ndodhur një ndërhyrje ose një incident tjetër kriminal, kjo zakonisht do të jetë:-
    - Regjistrimi ose të dhënat e krijimit të skedarëve që tregojnë se dikush është qasur në mënyrë të gabuar,
    - krijimet,

	• ndryshimet, • fshirja apo kopjimi i skedarëve ose egjistrimeve; • cilësimet e ndryshuara të sistemit; • shtimet ose ndryshimet e llogarive ose lejeve të përdoruesve. 21. Organizatës viktimë duhet t'i kërkohet të sigurojë që veprimet e saj të mos bëhen pa dashje ose pa nevojë; • Të mos ndryshojë të dhënat e ruajtura në mënyrë që mund të pengojë reagimin ndaj incidentit ose hetimin e mëvonshëm penal; • skedarët përkatës nuk duhet të fshihen, nëse është e mundur; shmangni modifikimin e të dhënave ose nëse është absolutisht e nevojshme për të ndryshuar të dhënat, mbani një regjistër auditimi se si dhe kur është modifikuar informacioni. *Kompania mund të bëjë një "imazh mjekoligjor" të kompjuterëve të prekur, i cili do të ruajë një regjistrim të sistemit në kohën e incidentit për analiza të mëvonshme dhe potencialisht për përdorim si provë në gjyq - Prokuroria/CCIU/DFU duhet të informohet për këtë veprim.*
Prokuroria: ***Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.***	**Në shumicën e rasteve që përfshijnë biznese, CCIU/DFU do të marrë përsipër hetimin në këtë fazë të udhëzuar nga prokuroria, megjithatë nëse kjo mbështetje nuk është e disponueshme, mund t'ju duhet të merrni parasysh fazat e mëposhtme të veprimit:** **Pajisja(/-et) e Ndezur** – Shkoni te 22. **Pajisja(/-et) e Fikur** – Shkoni te 30.
Prokuroria: ***Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.*** ***MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT***	**MOS E FIKNI PAJISJEN** Kjo do të ndryshojë provat, mund edhe të dëmtojë punën e viktimës. 22. 10. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi; 23. Nëse provat shfaqen dukshëm në ekran, shkrepni fotografi dhe mbani shënime për çdo material në ekranin e kompjuterit dhe programet e shfaqura në task bar; **Vetëm inspektim vizual** Mos u tundoni të lëvizni në kompjuter duke përdorur mausin ose tastierën.

E rëndësishme: ***Ruajtja dhe mbledhja e të dhënave përfshirë të dhënat digjitale është e rëndësishme***	24. Kërkoni të gjithë karikuesit ose manualet për pajisjen; 25. Pyetni Viktimën për fjalëkalimin dhe/ose numrin PIN të pajisjes dhe veçori të tjera sigurie si ato biometrike apo, në rastin e shifrimit, pyetni viktimën për fjalëkalimin/frazëkalimin dhe mbani regjistrim të detajeve. 26. Për të Shmangur Ndryshime në Largësi të të Dhënave – konsideroni izolimin e pajisjes nga Ethernet, Wi-Fi apo rrjeti i komunikimit. Me një pajisje celulare apo laptop, nëse jeni kompetent, konsideroni ndryshimin në "airplane mode" dhe regjistroni veprimet;
Qasja në Largësi ose Të Dhënat në Largësi mund të shkaktojnë ndryshime	27. Nuk jeni të sigurt për mbylljen e pajisjes apo shkëputjen e rrymës? **Së pari dhe urgjentisht konsultohuni me pronarin e biznesit & Menaxherin e Rrjetit përpara shkëputjes së menjëhershme të pajisjeve ose rrjetave nga burimi i energjisë,** Nëse nuk jeni të sigurt apo kompetentë për të kryer veprimet në pikën 13 ose 14, kërkoni ndihmë nga një teknik me përvojë – CCIU/DFU.
Sulm nga Programe Keqdashëse – Mund të fshihen apo korruptohen të dhëna.	28. Nëse ka tregues që kompjuteri ka të instaluara programe keqdashëse të cilat po fshijnë apo korruptojnë të dhëna nga hard disku, **konsultohuni urgjentisht me pronarin e biznesit & Menaxherin e Rrjetit përpara shkëputjes së menjëhershme të pajisjeve ose rrjetave nga burimi i energjisë,** në rastin e një laptopi ose celulari hiqni edhe baterinë. Regjistroni arsyen dhe veprimet që keni marrë. 29. Shkoni te **Sekuestrimi i Pajisjes**.
Pajisja e Fikur? ***Prokuroria:*** ***Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.*** ***Të japë udhëzime për sekuestrimin, paketimin dhe etiketimin si duhet të pajisjeve***	**MOS E NDIZNI** kjo do të ndryshojë provat. 30. Pyetni viktimën për fjalëkalimet, përcaktoni nëse pajisja është e kriptuar, pyetni viktimën për fjalëkalimin/frazëkalimin; 31. Siguroni karikuesin dhe manualet e pajisjes. **MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT** 32. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi. 33. Shkoni te **Sekuestrimi i Pajisjes**.

Pajisjet për Ruajtjen e të Dhënave dhe Mediave: ***Shembuj të këtyre pajisjeve përfshijnë, Hard Disqe (USB/ Wireless) USB Memory sticks, DVD, karta SD etc.***	34. Nëse pajisja është e ndezur ose e lidhur me një kompjuter 'të ndezur' në linjë, atëherë çdo shkëputje mund të sjellë ndryshime në të dhënat dhe/ose të shkaktojë humbjen e të dhënave. Merruni me pajisjen si në Veprimin 23-29. 35. Nëse pajisja është e izoluar dhe/ose e fikur veproni me pajisjen si te 30-33. 36. Shkoni te **Sekuestrimi i Pajisjes**.
Të Dhënat e Komunikimit të Telefonave Inteligjentë ose Pajisjeve të Lëvizshme: ***(IMEI - Identiteti Ndërkombëtar i Pajisjeve Celulare)*** ***IMSI - Identiteti Ndërkombëtar i pajtimtarit celular)*** ***Prokuroria po lëshon Urdhër për zbulimin e komunikimit telefonik nga operatori telefonik kombëtar për numrin e identifikuar të telefonit dhe më shumë informacion për numrin IMEI***	37. Siguroni nga viktima identifikuesit e pajisjes: • Numrin e telefonit • numrin IMEI • numrin IMSI; 38. Miratim me shkrim nga viktima për të siguruar të dhënat e komunikimit nga CSP Operatori i Shërbimeve të Komunikimit dhe/ose Operatori i Shërbimeve të Internetit. 39. Nëse është i nevojshëm sekuestrimi i telefonit - Shkoni te **Sekuestrimi i Pajisjes**.
Sekuestrimi i Pajisjes: ***PARALAJMËRIM – Mund të keni nevojë të mblidhni prova forensike të tjera përfshirë gjurma gishtash, mostra biologjike, ADN, etc. nga pajisjet. Këshillohuni me efektivët kriminalistikë të skenës së krimit për të ruajtur provat dhe integritetin e të dhënave në pajisje.***	40. Informoni viktimën pse po sekuestrohet pajisja dhe për sa kohë; 41. Merrni miratim me shkrim nga viktima për ekzaminim mjekoligjor të pajisjes; 42. Sekuestroni dhe Paketoni pajisjen sipas PSO/Ligjit; 43. Merrni në konsideratë që të kërkoni kompjutera të tjerë ose pajisje të tjera për ruajtje të dhënash që mund të përmbajnë kopje (backup) të pajisjeve; 44. Paketojeni pajisjen në mënyrë që të mos dëmtohet apo të deformohet fizikisht; 45. Paketojeni pajisjen në qese apo kuti provash; 46. Materialet e rrezikshme në pajisje duhet të detajohen në paketim dhe të informohet DFU.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Ky proces duhet të jetë i shpejtë me qëllim që të mos humbasin prova***	47. Dorëzojini provat te një objekt i sigurt i zbatimit të ligjit ose laborator provash digjitale sa më shpejt të jetë e mundur; 48. Mbroni nga temperaturat ekstreme, elektriciteti statik, fushat magnetike apo lagështia. 49. Mbani regjistrim auditimi për vazhdimësinë e provave.

Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Urdhri nga prokuroria duhet të konkretizojë se për çfarë provash duhet të kryhet kërkimi.*** ***Urdhri duhet të ketë përshkrimin dhe numri serial të saktë të secilës prej provave materiale***	50. Informoni për shkeljet Penale të identifikuara dhe Procedurat e Ndërmarra. 51. Merrni autorizim/Urdhër nga prokuroria për hetim të mëtejshëm.
Prokuroria mund të ndjekë procesin e kriminalistikës digjitale dhe nxjerrjes së provave digjitale	52. Nëse pajisjet janë sekuestruar për Imazhim ose Ekzaminim Digjital Mjekoligjor; informoni DFU për materialet e sekuestruara dhe vendimet hetimore të prokurorisë.

Hetimi i Krimeve që Përfshijnë Media Digjitale - Kompjuterë, Laptopë dhe Pajisje për Ruajtjen e të Dhënave/Mediave

HETIMI I KRIMEVE QË PËRFSHIJNË MEDIAN DIGJITALE – KOMPJUTERË, LAPTOPË

Kompjuterët e mediave digjitale dhe pajisjet e ruajtjes së të dhënave do të përmbajnë prova digjitale.

Provë digjitale është çdo informacion ose e dhënë me vlerë për një hetim që ruhet, merret ose transmetohet nga një pajisje elektronike. Mesazhet e çastit, emailet, skedarët, fotografitë dhe videot dhe kërkimet në internet janë disa nga llojet më të zakonshme të provave digjitale.

Të dyshuarit për krime kompjuterike ose krime të aktivizuara me kompjuter do të lënë një gjurmë kriminalistike digjitale në pajisjen e tyre dhe pajisjen e viktimës.

Prova Digjitale/Veprimet e Prokurorisë	Procesi hetimor
Çështja i raportohet prokurorisë: ***Prokuroria:*** ***Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar.***	**Kryeni Hetimin Penal për të identifikuar:** • Qëllimin kriminal; • Vendndodhjen dhe kohën e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; • Provat e krimit.
Raporti me informacion rreth çështjes i dorëzohet prokurorisë. Prokuroria: - ***Identifikon veprën penale që duhet të hetohet.*** - ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimin kriminalistik të pajisjeve.***	1. Siguroni skenën; 2. Mos e lejoni të dyshuarin pranë ndonjë pajisjeje ose burimi energjie; 3. Identifikoni autoritetin ligjor për sekuestrimin e provave; 4. Sekuestroni pajisjet në përputhje me PSO për sekuestrimin e provave; 5. Sigurohuni që pajisjet e sekuestruara të mos ekspozohen ndaj temperaturave ekstreme, elektricitetit statik, fushave magnetike ose lagështisë; 6. Regjistroni detajet e pajisjes dhe vendndodhjen dhe gjendjen në të cilën është gjetur;

E rëndësishme: **Ruajtja dhe mbledhja e provave, përfshirë edhe provat digjitale, është e rëndësishme.** *A po ndodh krimi tani apo ka ndodhur tashmë? A ka këtu ndonjë element që është kritik për kohën, p.sh. të dhënat po fshihen nga distanca, kërcënim për jetën?*	7. Fotografoni ose filmoni pajisjen ku është gjetur; 8. Mbani shënime se ku është gjetur dhe nga kush është konfiskuar; 9. Mbani një zinxhir të kujdestarisë; 10. Merrni parasysh informimin e prokurorisë, CCIU dhe DFU nëse ka ndikime dhe rreziqe të rëndësishme për këtë krim.
Statusi i Pajisjes: ***A është Pajisja Elektronike/ Digjitale e Ndezur apo e Fikur?***	**Pajisja është e Ndezur** – Shkoni te 11. **Pajisja është e Fikur** – Shkoni te 20.
Pajisja është e Ndezur: ***SHËNIM – Shumë pajisje kompjuterike kursejnë energji duke fikur ekranet apo duke u kthyer në gjendje gjumi pas njëfarë kohe të përcaktuar. Pavarësisht nga statusi i ekranit, pajisja ka të ngjarë të jetë ende aktive; veprime si ngritja e kapakut të një laptopi mund ta rikthejnë një pajisje në punë.*** **MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT**	11. Përcaktoni nëse pajisja është e ndezur apo e fikur; • Kërkoni dritat; • Dëgjo për tinguj; • Prekni për dridhje ose nxehtësi; • Pyetni nëse pajisja është e ndezur; • MOS E FIKNI PAJISJEN Kjo do të ndryshojë provat. 12. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi. 13. Nëse ka shfaqje të dukshme në ekran, shkrepni fotografi dhe mbani shënime për çdo material në ekranin e kompjuterit dhe programet e shfaqura në task bar; **Vetëm inspektim vizual** Mos u tundoni të lëvizni në kompjuter duke përdorur mausin ose tastierën. 14. Sekuestroni të gjithë karikuesit ose manualet për pajisjen; 15. Pyetni të dyshuarin për fjalëkalimin e kompjuterit identifikoni biometrikën apo veçori sigurie me kriptim; kërkoni dhe regjistroni fjalëkalimin/frazëkalimin;

Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet. ***Të japë udhëzime për sekuestrimin, paketimin dhe etiketimin si duhet të pajisjeve***	16. *Parandaloni ndryshimin e të Dhënave*; **nëse jeni kompetent**, merrni në konsideratë izolimin e pajisjes nga rrjetet Ethernet dhe Wi-Fi. Me një laptop merrni parasysh ndryshimin në airplane mode – regjistroni veprimet; 17. Nuk jeni të sigurt për mbylljen e pajisjes apo shkëputjen e rrymës? Nëse nuk jeni të sigurt apo kompetentë për të kryer veprimet në pikën 15 ose 16, kërkoni ndihmë nga një teknik me përvojë – CCIU/DFU. 18. Nëse ka tregues që kompjuteri ka të instaluara programe keqdashëse të cilat po fshijnë apo korruptojnë të dhëna nga hard disku, shkëputeni pajisjen menjëherë nga burimi i rrymës, në rastin e një laptopi ose celulari hiqni edhe baterinë. Regjistroni arsyen dhe veprimet që keni marrë; 19. Shkoni te **Sekuestrimi i Pajisjes**.
Pajisja është e Fikur? ***SHËNIM – Shumë pajisje kompjuterike kursejnë energji duke fikur ekranet apo duke u kthyer në gjendje gjumi pas njëfarë kohe të përcaktuar. Pavarësisht nga statusi i ekranit, pajisja ka të ngjarë të jetë ende aktive; veprime si ngritja e kapakut të një laptopi mund ta rikthejnë një pajisje në punë.***	**MOS E NDIZNI** provat do të ndryshohen. 20. Pyesni të dyshuarin për fjalëkalimin; 21. Sekuestroni të gjithë karikuesit ose manualet për pajisjen; 22. Përcaktoni nëse pajisja është e kriptuar nëse është kërkojini të dyshuarit fjalëkalimin/frazëkalimin; MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi.
Pajisjet e Ruajtjes së të Dhënave dhe Mediave: ***Shembuj të këtyre pajisjeve përfshijnë, Hard Disqet (USB/Wireless) USB Memory sticks, DVD, kartat SD etc.***	23. Nëse pajisja është e ndezur ose e lidhur me një kompjuter 'të ndezur' në linjë, atëherë çdo shkëputje e një pajisjeje të lidhur mund të sjellë ndryshime në të dhënat dhe/ose të shkaktojë humbjen e të dhënave. Merruni me pajisjen si në Veprimin. Merruni me pajisjen si në Veprimin 11-19; 24. Nëse pajisja është e izoluar dhe/ose e fikur veproni me pajisjen si te Veprimi 20-22.

Sekuestrimi i pajisjes: ***PARALAJMËRIM – Mund të keni nevojë të mblidhni prova forensike të tjera përfshirë gjurma gishtash, mostra biologjike, ADN, etc. nga pajisjet. Këshillohuni me efektivët kriminalistikë të skenave të krimit për 27-31 për të ruajtur provat dhe integritetin e të dhënave në pajisje.***	25. Informoni të dyshuarin që pajisja po sekuestrohet dhe pse; 26. Merrni miratim me shkrim nga i dyshuari për ekzaminim kriminalistik të pajisjes. 27. Sekuestrojeni dhe Paketojeni pajisjen sipas PSO/Ligjit; 28. Merrni në konsideratë sekuestrimin e kompjuterave të tjerë ose pajisjeve të tjera për ruajtje të dhënash që mund të përmbajnë kopje (backup) të pajisjeve; 29. Paketojeni pajisjen në mënyrë që të mos dëmtohet apo të deformohet fizikisht; 30. Paketojeni pajisjen në qese apo kuti provash; 31. Materialet e rrezikshme në pajisje duhet të detajohen në paketim dhe të informohet DFU.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajiseve të sekuestruara. ***Ky proces duhet të jetë i shpejtë me qëllim që të mos humbasin prova***	32. Dorëzojini provat te një objekt i sigurt i zbatimit të ligjit ose laborator provash digjitale sa më shpejt të jetë e mundur; Ruajtja e pajisjeve do të jetë te DFU; 33. Mbroni nga temperaturat ekstreme, elektriciteti statik, fushat magnetike apo lagështia; 34. Mbani regjistrim auditimi për vazhdimësinë e provave.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajiseve të sekuestruara. ***Urdhri nga prokuroria duhet të konkretizojë se për çfarë provash duhet të kryhet kërkimi.*** ***Urdhri duhet të ketë përshkrimin dhe numri serial të saktë të secilës prej provave materiale***	35. Informoni për shkeljet Penale të identifikuara dhe Procedurat e Ndërmarra; 36. Objektet sekuestrohen; 37. Merrni autorizim/Urdhër për hetim të mëtejshëm.
Prokuroria mund të ndjekë procesin e kriminalistikës digjitale dhe nxjerrjes së provave digjitale	38. Informoni për materialet e sekuestruara dhe vendimet e prokurorisë.

Hetimi i Krimeve që Përfshijnë Media Digjitale – Smartphone, Tableta dhe Pajisje të lëvizshme

HETIMI I KRIMEVE QË PËRFSHIJNË MEDIA DIGJITALE – SMARTPHONE, TABLETA DHE PAJISJE TË LËVIZSHME.

Prova digjitale është çdo informacion ose e dhënë me vlerë për një hetim që ruhet, merret ose transmetohet nga një pajisje elektronike. Mesazhet me tekst, SMS, kontaktet, thirrjet drejt dhe nga një pajisje, emailet, fotografitë dhe videot dhe kërkimet në internet janë disa nga llojet më të zakonshme të provave digjitale që gjenden në Smartphone, Tableta dhe pajisje të tjera celulare.

Pajisjet e të dyshuarit që lidhen me pajisjen e viktimës do të lënë një gjurmë forensike në një sërë fazash të komunikimit.

Provat Digjitale / Veprimet e Prokurorisë	Procesi hetimor
Çështja i raportohet prokurorisë: ***Prokuroria:*** ***Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar.*** **Kriminelët tani lënë gjurmë digjitale:** ***Telefoni ose pajisja e lëvizshme e një të dyshuari do të përmbajë skedarë që japin informacion kritik si pika prove në një hetim penal.***	• Qëllimin kriminal; • Vendndodhjen dhe kohën e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; Provat e krimit.
Raporti me informacion rreth çështjes i dorëzohet prokurorisë. Prokuroria: - ***Identifikon veprën penale që duhet të hetohet.***	1. Siguroni skenën; 2. Mos e lejoni të dyshuarin pranë ndonjë pajisjeje ose burimi energjie; 3. Identifikoni autoritetin ligjor për sekuestrimin e provave; 4. Sekuestroni pajisjet në përputhje me procedurat normale për sekuestrimin e provave;

- ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimin kriminalistik të pajisjeve.***	5. Sigurohuni që pajisjet e sekuestruara të mos ekspozohen ndaj temperaturave ekstreme, elektricitetit statik, fushave magnetike ose lagështisë; 6. Regjistroni detajet e pajisjes dhe vendndodhjen dhe gjendjen në të cilën është gjetur; 7. Fotografoni ose filmoni pajisjen ku është gjetur; 8. Mbani shënime se ku është gjetur dhe nga kush është konfiskuar; 9. Mbani një zinxhir të kujdestarisë; 10. Merrni parasysh informimin e prokurorisë, CCIU dhe DFU nëse ka ndikime dhe rreziqe të rëndësishme për këtë krim.
Statusi i Pajisjes: ***Është Pajisja Elektronike/ Digjitale e Ndezur apo e Fikur?***	**Pajisja(/-et) e Ndezur** – Shkoni te 11. **Pajisja(/-et) e Fikur** – Shkoni te 19.
Device Powered On: ***SHËNIM – Shumë pajisje të lëvizshme kursejnë energji duke fikur ekranet pas një kohe të caktuar. Pavarësisht nga statusi i ekranit, pajisja ka të ngjarë të jetë ende aktive.*** **MOS NDËRMERRNI ASNJË VEPRIM QË MUND TË NDRYSHOJË TË DHËNAT** ***Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet.*** ***Prokuroria duhet të japë udhëzime për sekuestrimin, paketimin dhe etiketimin si duhet të pajisjeve.***	11. Përcaktoni nëse pajisja është e ndezur apo e fikur; • Kërkoni dritat; • Dëgjo për tinguj; • Prekni për dridhje ose nxehtësi; • Pyetni nëse pajisja është e ndezur; • MOS E FIKNI PAJISJEN Kjo do të ndryshojë provat. 12. Në rast se kryhen ndryshime, aksidentalisht apo qëllimisht, regjistroni orën, datën dhe veprimin me detajet e ndryshimit që ndodhi. 13. Sekuestroni çdo karikues apo manual për pajisjen; 14. Pyetni të dyshuarin për fjalëkalimin dhe/ose numrin PIN dhe veçori të tjera sigurie të telefonit, mbani regjistrime të të dhënave; 15. Parandaloni lëshimin e të dhënave – Izolojeni pajisjen nga rrjetet celulare dhe Wi-Fi duke përdorur Qese Faraday apo duke e mbështjellë me letër alumini; SCFU për të ndihmuar këtu; 16. **Nëse jeni kompetent** është thelbësore ta parandaloni telefonin që të lidhet me një rrjet, merrni në konsideratë që ta vendosni telefonin në “airplane mode” dhe të regjistroni veprimet;

	17. **<u>Nëse nuk jeni kompetent</u>** kërkojini ndihmë një tekniku me përvojë nga CCIU/DFU. 18. Shkoni te **Sekuestrimi i Pajisjes**.
Prokuroria duhet të këshillojë që, nëse kompjuteri është i fikur, ai të mos ndizet. ***Prokuroria duhet të japë udhëzime për sekuestrimin, paketimin dhe etiketimin si duhet të pajisjeve.***	**SHËNIM: Shumë pajisje të lëvizshme kursejnë energji duke fikur ekranet pas një kohe të caktuar. Pavarësisht nga statusi i ekranit, pajisja ka të ngjarë të jetë ende aktive.** **<u>MOS E NDIZNI</u> Provat do të ndryshohen.** 19. Pyetni të dyshuarin për fjalëkalimin dhe/ose numrin PIN; 20. Sekuestroni çdo karikues apo manual për pajisjen.
Sekuestrimi i Pajisjes: ***PARALAJMËRIM – Mund të keni nevojë të mblidhni prova forensike të tjera përfshirë gjurma gishtash, mostra biologjike, ADN, etc. nga pajisjet. Këshillohuni me efektivët forensikë të skenave të krimit për t'ju ndihmuar me 22-26 për të ruajtur provat dhe integritetin e të dhënave në pajisje.***	21. Informoni të dyshuarin që po sekuestrohet pajisja dhe pse; 22. Merrni miratim me shkrim nga i dyshuari për ekzaminim forensik të pajisjes. 23. Sekuestroni dhe Paketoni pajisjen sipas PSO/Ligjit; 24. Merrni në konsideratë që të kërkoni kompjutera të tjerë ose pajisje të tjera për ruajtje të dhënash që mund të përmbajnë kopje (backup) të pajisjes; 25. Paketojeni pajisjen në mënyrë që të mos dëmtohet fizikisht apo të deformohet; 26. Paketojeni pajisjen në qese apo kuti provash; 27. Materiale të rrezikshme në pajisje? – Detajojini në paketim dhe informoni DFU.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Ky proces duhet të jetë i shpejtë me qëllim që të mos humbasin prova***	28. Dorëzojini provat te një objekt i sigurt i zbatimit të ligjit ose laborator provash digjitale sa më shpejt të jetë e mundur; Magazinimi i pajisjeve do të bëhet te DFU; 29. Mbroni nga temperaturat ekstreme, elektriciteti statik, fushat magnetike apo lagështia; 30. Mbani regjistrim auditimi për vazhdimësinë e provave.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara.	31. Informoni për shkeljet Penale të identifikuara dhe Procedurat e Ndërmarra; 32. Merrni autorizim/Urdhër për hetim të mëtejshëm.

Urdhri nga prokuroria duhet të konkretizojë se për çfarë provash duhet të kryhet kërkimi. ***Urdhri duhet të ketë përshkrimin dhe numri serial të saktë të secilës prej provave materiale***	
Prokuroria mund të ndjekë procesin e kriminalistikës digjitale dhe nxjerrjes së provave digjitale	33. Informoni për materialet e sekuestruara dhe vendimet hetimore të prokurorisë.

Administrimi dhe sekuestrimi i provave që lidhen me Hetimin e Imazheve të Abuzimit të Fëmijëve (Pornografisë së Fëmijëve) që mbahen në Media Digjitale

Sekuestrimi i Mediave Digjitale - Hetimi i imazheve të abuzimit me fëmijët (pornografia e fëmijëve).

Media digjitale do të përmbajë prova digjitale. Provë digjitale është çdo informacion ose e dhënë me vlerë për një hetim që ruhet, merret ose transmetohet nga një pajisje elektronike. Mesazhet me tekst, emailet, fotografitë dhe videot, skedarët, dokumentet dhe kërkimet në internet janë disa nga llojet më të zakonshme të provave digjitale.

Të dyshuarit në hetimet e shfrytëzimit të fëmijëve shpesh përdorin komunikimin privat, ndarjen e skedarëve privat (P2P), teknikat e ruajtjes së skedarëve dhe kriptimin për të maskuar dhe fshehur veprimet e tyre me bashkëpunëtorët.

Prokuroria duhet të kontaktohet sa më shpejt që të jetë e mundur dhe t'i jepet një përmbledhje e krimit, ndikimit, çdo personi të cenueshëm dhe çdo rrezik.

Provat Digjitale/Veprimet e Prokurorisë	Procesi hetimor
Çështja i raportohet prokurorisë: ***Prokuroria:*** ***Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar.***	**Hetim Penal për të identifikuar:** • Qëllimin kriminal; • Vendndodhjen dhe kohën e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; • Provat e krimit.
Raporti me informacion rreth çështjes i dorëzohet prokurorisë. Prokuroria: - ***Identifikon veprën penale që duhet të hetohet.*** - ***Identifikon nëse provat mund të merren në format elektronik ose në letër*** - ***Identifikon autoritetin ligjor që mban provat, Përgatit Urdhrin për ruajtjen dhe zbulimin e të dhënave***	1. Siguroni skenën; 2. Mos e lejoni të dyshuarin pranë asnjë pajisjeje apo burimi energjie; 3. Sekuestroni provat – Identifikoni autoritetin ligjor; 4. Sekuestroni pajisjet sipas PSO-ve normale të sekuestrimit të provave; 5. Sigurohuni që pajisjet e sekuestruara të mos ekspozohen ndaj temperaturave ekstreme, elektricitetit statik, fushave magnetike apo lagështisë;

- ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimin kriminalistik të pajisjeve.*** ***Shtesë:*** ***Prokuroria mund të kërkojë mbledhjen dhe regjistrimin e të dhënave nga Burime të Hapura (OSINT)*** ***E rëndësishme:*** ***Është e rëndësishme që provat, përfshirë provat elektronike, të ruhen dhe të mblidhen si duhet.*** *A po ndodh krimi tani apo ka ndodhur tashmë? A ka këtu ndonjë element që është kritik për kohën, p.sh. të dhënat po fshihen nga distanca, kërcënim për jetën?*	6. Regjistroni detajet e pajisjes dhe vendndodhjen dhe gjendjen në të cilat është gjetur; 7. Fotografoni ose filmoni pajisjen në vendin e gjetjes; 8. Mbani shënime se ku gjendet pajisja dhe prej kujt sekuestrohet; 9. Mirëmbani një zinxhir kujdestarie.
Statusi i Pajisjes: ***Është Pajisja Elektronike/ Digjitale e Ndezur apo e Fikur?***	**Referohuni te:** **Sekuestrimi i Mediave Digjitale – Telefonat Inteligjentë dhe pajisje të tjera të lëvizshme.** **Sekuestrimi i Mediave Digjitale – Kompjutera, Laptopë & Pajisje të Ruajtjes së të Dhënave/Mediave.**
Prokuroria mund të lëshojë urdhër për sekuestrimin e të dhënave kompjuterike ose të kryejë procedura kriminalistike për të dhëna në kohë reale **E rëndësishme: Programe aplikative Peer-to-Peer (P2P):** ***P2P përdoret shpesh nga të dyshuarit për të shpërndarë Imazhe të Shfrytëzimit të Fëmijëve; individët në këto rrjeta mirëmbajnë "biblioteka" imazhesh për t'i ndarë me të tjerët.***	10. Kontrolloni për programe P2P të shfaqura në ekranin e pajisjes ose në toolbar-in e pajisjes; 11. Pyetni të dyshuarin për adresat IP, ID-të/ fjalëkalimet e llogarive dhe çdo veçori tjetër sigurie të rrjetit P2P si kriptimi dhe mbani regjistrim të detajeve. **Visual inspection only** **Do Not be tempted to navigate the computer using the mouse or keyboard.**

Programe të njohura P2P janë Gnutella, Fast-Track, BitTorrent, eDonkey, Limewire dhe Freenet.	
Kriptimi: ***Të dyshuarit e përfshirë në mbledhjen dhe shpërndarjen e Imazheve të Abuzimit të Fëmijëve (Pornografisë së Fëmijëve) shpesh përdorin kriptim.*** ***Prokuroria mund të lëshojë urdhër për të kryer procedura kriminalistike për të dhëna në kohë reale*** ***Identifikon se cili profil eksperti të përfshijë në procesin e identifikimit dhe sekuestrimit të provave elektronike***	**Nëse pajisja është e NDEZUR – MOS E FIKNI** **Provat mund të humbasin – kontaktoni CCIU/DFU.** 12. Pyesni të dyshuarin për fjalëkalimin/ frazëkalimin; 13. Nëse ka pamje të dukshme në ekran, shkrepni fotografi dhe mbani shënime për çdo material në ekranin e kompjuterit dhe programet e shfaqura në task bar; **Vetëm inspektim vizual** Mos u tundoni të lëvizni në kompjuter duke përdorur mausin ose tastierën. 14. Vetëm një **person** k**ompetent** ose Ekzaminues Forensik Digjital **i akredituar** duhet të ndërmarrë një Ekzaminim Digjital të Drejtpërdrejtë (‘Live’). Kontaktoni CCIU dhe DFU.
Prokuroria: - ***Identifikon nëse provat mund të merren në format elektronik ose në letër*** - ***Identifikon autoritetin ligjor që mban provat, Përgatit Urdhrin për ruajtjen dhe zbulimin e të dhënave*** - ***Nëse një pjesë e provave janë të ruajtura në kompjuter, Lëshon Urdhrin për sekuestrimin e pajisjes dhe Urdhrin për ekzaminimn kriminalistik të pajisjeve.*** - ***Prokuroria duhet të lëshojë urdhër për sekuestrimin e të dhënave kompjuterike, për kryerjen e procedurave***	15. Kërkoni për Media Sociale/programe për IRC në ekranin e pajisjes ose të shfaqura në toolbar-in e pajisjes; 16. Pyetni të dyshuarin për ID-të/fjalëkalimet e llogarive dhe çdo veçori sigurie të metodës të komunikimit si kriptimi dhe mbani regjistrim të detajeve. **Vetëm inspektim vizual** Mos u tundoni të lëvizni në kompjuter duke përdorur mausin ose tastierën.

kriminalistike për të dhëna në kohë reale ose për sekuestrimin e të tëra pajisjeve që kanë prova elektronike **Metoda e Komunikimit:** ***Faqe Mediash Sociale si Facebook, Twitter etj. janë metoda komunikimi për "grooming" në Pornografinë e Fëmijëve.*** ***IRC (Internet Relay Chat) përdoret ende si komunikim privat ndërmjet të Dyshuarve për Shfrytëzim Fëmijësh.*** ***Programe të njohura për IRC software janë Freenode, IRCNet, QuakeNet, EFNet, Undernet & Rizon.***	
Pajisjet e Ruajtjes së të Dhënave dhe Mediave:	**Referojuni:** **Sekuestrimi i Mediave Digjitale –** Kompjutera, Laptopë & Pajisje të Ruajtjes së të Dhënave/Mediave.
Sekuestrimi i Pajisjes(/-eve): ***PARALAJMËRIM – Mund të keni nevojë të mblidhni prova forensike të tjera përfshirë gjurma gishtash, mostra biologjike, ADN, etc. nga pajisjet. Këshillohuni me efektivët forensikë të skenave të krimit për të ruajtur provat dhe integritetin e të dhënave në pajisje.***	17. Informoni të dyshuarin që po sekuestrohet pajisja dhe pse. 18. Merrni miratim me shkrim nga i dyshuari për ekzaminim mjekoligjor të pajisjes. 19. Sekuestroni dhe Paketoni pajisjen sipas PSO/ Ligjit; 20. Merrni në konsideratë që të kërkoni kompjutera të tjerë ose pajisje të tjera për ruajtje të dhënash që mund të përmbajnë kopje (backup) të pajisjes; 21. Paketojeni pajisjen në mënyrë që të mos dëmtohet fizikisht apo të deformohet; 22. Paketojeni pajisjen në qese apo kuti provash; 23. Materialet e rrezikshme në pajisje duhet të detajohen në paketim dhe të informohet DFU.

Prokuroria duhet të lëshojë urdhër për ekzaminimin kriminalistik të pajisjeve të sekuestruara. ***Ky proces duhet të jetë i shpejtë me qëllim që të mos humbasin prova***	24. Dorëzojini provat te një objekt i sigurt i zbatimit të ligjit ose laborator provash digjitale sa më shpejt të jetë e mundur; 25. Mbroni nga temperaturat ekstreme, elektriciteti statik, fushat magnetike apo lagështia; 26. Mbani regjistrim Auditimi për vazhdimësinë e provave.
Prokuroria duhet të lëshojë një urdhër për ekzaminim kriminalistik të pajisjeve të sekuestruara. ***Urdhri nga prokuroria duhet të konkretizojë se për çfarë provash duhet të kryhet kërkimi.*** ***Urdhri duhet të ketë përshkrimin dhe numri serial të saktë të secilës prej provave materiale***	27. Informoni për shkeljet Penale dhe Procedurat e Ndërmarra; 28. Merrni autorizim/Urdhër për hetim të mëtejshëm.
	29. Informoni për krimin për këshilla dhe ndihmë të specializuar për hetimin. 30. Informoni për materialin e sekuestruar dhe vendimet e prokurorisë.

Marrja e të dhënave nga operatorët kombëtarë dhe ndërkombëtarë të shërbimeve të Internetit

Marrja e të dhënave nga operatorët kombëtarë dhe ndërkombëtarë të shërbimeve të Internetit	
Duke qenë se hetimi i krimit kibernetik nga organet e zbatimit të ligjit shpesh nuk është efektiv pa bashkëpunimin e operatorëve të shërbimeve të internetit, është thelbësore që të dyja të bashkëpunojnë me njëra-tjetrën në një mënyrë efikase. *Rolet e të dyjave janë të ndryshme: zbatimi i ligjit duhet të respektojë ligjin, ndërsa operatorët e shërbimeve duhet t'u ofrojnë përdoruesve aftësinë për të komunikuar.* *Pyetja me të cilën përballen shumë vende është se si të dyja mund të bashkëpunojnë më mirë me njëri-tjetrin për ta bërë internetin më të sigurt, duke respektuar në të njëjtën kohë rolet e tyre të ndryshme dhe të drejtat themelore të përdoruesve. Dhe shumë e rëndësishme se si ofruesit e shërbimeve të internetit mund të mbështesin hetimin penal të krimit kibernetik dhe krimet e mundësuara kibernetike.*	
Provat Digjitale/Veprimet e Prokurorisë	**Procesi**
Çështja i raportohet prokurorisë: ***Prokuroria:*** ***Në këtë çast, prokuroria informohet për çështjen dhe prokurori i jep urdhër policisë gjyqësore për mbledhjen e informacionit rreth çështjes së raportuar.*** **Identifikon operatorin e shërbimeve të Internetit që mban të dhënat/provat për çështjen**	• Qëllimi kriminal; • Vendndodhja dhe koha e krimit; • Marrëdhëniet me viktimën/-at; • Marrëdhëniet me të dyshuarin/-it e tjerë; • Provat e krimit.
	Operator kombëtar i shërbimeve të Internetit **Operator i shërbimeve të Internetit nën juridiksionin e një shteti tjetër** **Operator ndërkombëtar i shërbimeve të Internetit (zakonisht ISP nën juridiksionin e ShBA)**

Të dhënat e mbajtura nga një operator kombëtar i shërbimeve të Internetit ***Prokuroria:*** - ***Identifikon veprën penale që duhet të hetohet.*** - ***Lëshon kërkesë për ruajtjen e të dhënave*** - ***Lëshon kërkesë për zbulimin e të dhënave (MLA)***	1. Identifikoni operatorin kombëtar të shërbimeve të Internetit; 2. Identifikoni adresën dhe personin përgjegjës për zbulimin e të dhënave të nevojshme 3. Kontrolloni nëse operatori i shërbimeve të Internetit ka tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 4. Krijoni dhe dërgoni kërkesën për ruajtjen dhe zbulimin e të dhënave 5. Analizoni të dhënat e marra 6. Vendosni nëse ato të dhëna mund të pranohen si prova
Të dhënat e mbajtura nga një operator i shërbimeve të Internetit nën juridiksionin e një shteti tjetër ***Prokuroria:*** - ***Identifikon veprën penale që duhet të hetohet.*** - ***Lëshon kërkesë për ruajtjen e të dhënave*** - ***Lëshon kërkesë për zbulimin e të dhënave (MLA)***	1. Identifikoni operatorin e shërbimeve të Internetit; 2. Identifikoni vendin/juridiksionin 3. Merrni informacionin nëse kemi marrëveshje dypalëshe për bashkëpunim dhe shkëmbim provash 4. Kontrolloni nëse operatori i shërbimeve të Internetit ka tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 5. Përgatitni kërkesën për ruajtjen e të dhënave 6. Dërgoni kërkesën për ruajtjen e të dhënave nëpërmjet një kanali zyrtar 7. Përdorni kanalin e policisë (pika kontaktuese 24/7) për dërgimin e kërkesës 8. Nisni procesin e MLA në mënyrë që të dhënat të zbulohen dhe të jenë të pranueshme 9. Analizoni të dhënat e marra
Të dhënat e mbajtura nga një operator ndërkombëtar i shërbimeve të Internetit ***Prokuroria:*** - ***Identifikon veprën penale që duhet të hetohet.***	1. Identifikoni operatorin ndërkombëtar të shërbimeve të Internetit; 2. Identifikoni adresën dhe personin përgjegjës për zbulimin e të dhënave të nevojshme 3. Kontrolloni nëse operatori i shërbimeve të Internetit ka tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes)

- ***Lëshon kërkesë për ruajtjen e të dhënave*** - ***Lëshon kërkesë për zbulimin e të dhënave (MLA)***	4. Kontrolloni politikën e operatorit për bashkëpunimin me agjencitë e zbatimit të ligjit 5. Krijoni dhe dërgoni një kërkesë për ruajtjen e të dhënave 6. Krijoni dhe dërgoni një kërkesë për zbulimin e të dhënave 7. Analizoni të dhënat e marra 8. Vendosni nëse ato të dhëna mund të pranohen si prova
	Kërkesa për ruajtje **Kërkesa për zbulimin e të dhënave (kërkesë MLA)**
Kërkesa për ruajtjen e të dhënave ***Shtojca 2***	1. Identifikoni operatorin ndërkombëtar të shërbimeve të Internetit; 2. Identifikoni adresën dhe personin përgjegjës për zbulimin e të dhënave të nevojshme 3. Kontrolloni nëse operatori i shërbimeve të Internetit ka tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 4. Kontrolloni politikën e operatorit për bashkëpunimin me agjencitë e zbatimit të ligjit 5. Përgatitni kërkesën për ruajtjen e të dhënave
Kërkesa për zbulimin e të dhënave (kërkesë MLA) ***Shtojca 3***	1. Identifikoni operatorin ndërkombëtar të shërbimeve të Internetit; 2. Identifikoni vendin/juridiksionin 3. Merrni informacionin nëse kemi marrëveshje dypalëshe për bashkëpunim dhe shkëmbim provash 4. Kontrolloni nëse operatori i shërbimeve të Internetit mban tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 5. Përgatitni kërkesën për ruajtjen e të dhënave

	6. Nisni procesin e MLA në mënyrë që të dhënat të zbulohen dhe të jenë të pranueshme. Përdorni kanalin e policisë (pika kontaktuese 24/7) për dërgimin e kërkesës (vetëm për të shpejtuar procesin e dërgimit të kërkesës) 7. Dërgoni kërkesën MLA nëpërmjet një kanali zyrtar (Ministrisë së Drejtësisë, Ministrisë së Jashtme)
	Të dhënat e pajtimtarit **Të dhënat e trafikut** **Të dhënat e përmbajtjes**
Të dhënat e pajtimtarit ***Prokuroria lëshon urdhër/kërkesë për zbulimin e të dhënave të pajtimtarit***	1. Identifikoni operatorin e shërbimeve të Internetit; 2. Identifikoni adresën dhe personin përgjegjës për zbulimin e të dhënave të nevojshme 3. Kontrolloni nëse operatori i shërbimeve të Internetit mban tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 4. Kontrolloni politikën e operatorit (ligjin nëse është operator kombëtar i shërbimeve të Internetit) për zbulimin e të dhënave te agjencitë e zbatimit të ligjit 5. Përgatitni kërkesën
Të dhënat e trafikut **Të dhënat e përmbajtjes** Prokuroria/gjykata po lëshon urdhër/kërkesë për zbulimin e të dhënave të Trafikut dhe Përmbajtjes	1. Identifikoni operatorin e shërbimeve të Internetit; 2. Identifikoni adresën dhe personin përgjegjës për zbulimin e të dhënave të nevojshme 3. Kontrolloni nëse operatori i shërbimeve të Internetit mban tipin e nevojshëm të të dhënave (sipas politikës së kompanisë, rregulloreve për mbrojtjen e të dhënave personale, politikës së ruajtjes) 4. Kontrolloni politikën e operatorit (ligjin nëse është operator kombëtar i shërbimeve të Internetit) për zbulimin e të dhënave te agjencitë e zbatimit të ligjit 5. Përgatitni kërkesën

FJALOR SHPJEGUES

Shifrim asimetrik	Përdoret një çelës publik për shifrimin, një çelës privat për deshifrimin.
Portë e Pasme	Kod keqdashës i përhapur që zakonisht futet dhe instalohet nga viruset, krimbat apo trojanët.
Bot	Term për një kompjuter të kompromentuar që është integruar në një botnet.
Botnet	Rrjet robotësh që fillimisht janë kompromentuar nga krimbat apo trojanët dhe më pas presin udhëzime.
C&C Server	Server për komandim dhe kontroll, për të kontrolluar botet.
Virus kompjuterik	Manipulon hapësirat e sistemit, programet apo mjediset e tyre jashtë kontrollit të përdoruesit.
Përmbajtës	Term për skedarë të shifruar.
Bullizmi Kibernetik	Shihni Ngacmimet Online
Përndjekja Kibernetike	Shihni Ngacmimet Online
DNS	Sistemi i emrave të domeneve (Domain Name System) përkthen emrin e kompjuterit apo URL e një faqeje web-i në një adresë IP.
Drive-by download	Shkarkim pa dashje/i pakuptuar i programeve keqdashëse gjatë vizitës së një faqeje.
Shpërndarës	Dikush që merr paketa, shkëmben etiketat dhe i përcjell paketat.
Drejtuesi i shpërndarësve	Organizon personat shpërndarës dhe ndan detyrat e tyre.
Shifrim	Proces që kthen tekst të lexueshëm në tekst të shifruar me një algoritëm kriptimi dhe zakonisht me një çelës sekret.
eTAN	Një pajisje e vogël elektronike që zëvendëson kodet (TAN) duke krijuar kode të reja në kohë reale. Gjatë futjes së të dhënave në një transaksion online, faqja e bankës gjeneron një numër kontrolli që futet nga klientët

	e tyre në pajisjet eTAN. Pajisja eTAN atëherë përgjigjet me një numër që i jep mundësi klientit të përfundojë transaksionin.
Exploit	Program ose varg komandash që shfrytëzojnë dobësi të caktuara dhe / ose parregullsi në funksionim të një programi tjetër.
Exploit ose zero-day exploit	Shfrytëzimi i një vrime sigurie në të njëjtën ditë ose përpara se dobësia të njihet publikisht quhet 0day exploit.
IMEI	Identiteti ndërkombëtar i pajisjes celulare - një numër serial 15-shifror që mund të përdoret për të identifikuar në mënyrë unike pajisjet celulare.
IMSI	Identiteti Ndërkombëtar i Abonentit Celular identifikon në mënyrë unike pajtimtarët e rrjetit. IMSI ruhet në një SIM (Moduli i Identitetit të Pajtimtarit). IMSI është një numër unik 15 shifror i caktuar ekskluzivisht për çdo kartë SIM në mbarë botën nga operatorët e rrjetit.
Aplikacionet në Internet	Modelet e ofrimit të softuerit si shërbim (SaaS) dhe fjalët dhe frazat në lidhje me faqet e Internetit, tregtinë elektronike
Adresa IP	Adresa e Protokollit të Internetit - Një numër unik që përcakton adresën e kompjuterëve dhe pajisjeve të tjera brenda një rrjeti IP.
iTAN	TAN i indeksuar, klientëve u kërkohet nga banka që të fusin një TAN të posaçëm nga listat e tyre të indeksuara me numrat e pozicioneve.
Letschka List	Një listë e të dhënave personale të individëve që kanë reaguar ndaj spam-it dhe veprojnë padashur për një grup kriminal P.sh.: Mushka Parash/Shpërndarës.
Programe keqdashëse	Programe me funksione dashakeqëse – Programe kompjuterike që kryejnë veprime të dëmshme të padëshiruara nga përdoruesit.
Ndërhyrësit e Ndërmjetëm	Sulmuesi ndodhet ndërmjet dy partnerëve të komunikimit, fizikisht apo logjikisht, pa u zbuluar që ai ka kontroll mbi trafikun e të dhënave ndërmjet dy ose më shumë pjesëmarrësve të rrjetit, dhe mund të lexojë dhe/ose të manipulojë informacionin sipas dëshirës.

Mobbing	I ngjashëm me Ngacmimet Online, por i përqendruar në vendin e punës
Mushkë parash	Mushkat e parave tërheqin fondet e marra në mënyrë të paligjshme si para të gatshme sapo paratë mbërrijnë në llogarinë e tyre dhe i dërgojnë ato jashtë vendit nëpërmjet shërbimeve të transfertave të parave.
mTAN	TAN-et celulare përdorin kanalin e SMS-ve.
Siguria e Rrjetave	Term që lidhet me sigurinë e rrjetit, përfshirë parandalimin e ndërhyrjeve, VPN-të dhe programet mbrojtëse të tipit firewall.
Online Harassment	Ngacmimi në Internet nganjëherë referohet si ngacmim kibernetik, ndjekje kibernetike ose trolling. Për shkak të aksesit më të madh në internet, ky krim po bëhet më i përhapur dhe mund të variojë nga thirrjet e thjeshta me nofka deri te një fushatë e vazhdueshme ngacmimi, duke përfshirë kërcënimet për vrasje dhe përdorimin e profileve të shumta false në internet.
P2P	Peer to Peer
Mushkë paketash	Mushkat e paketave shpërndajnë paketa.
Peer to Peer	Në një rrjet peer-to-peer (P2P), të gjithë kompjuterët janë të barabartë dhe mund të ofrojnë shërbime si dhe të përdorin shërbime.
Phishing	E-mail-i përdoret për të mashtruar marrësit me qëllim zbulimin e të dhënave të qasjes dhe fjalëkalimet në sistemin bankar online dhe në sistemet e tjera të pagesave.
Private key (secret key)	Një çelës shifrimi, vlera e të cilit nuk duhet të bëhet kurrë publike. Termi mund t'i referohet çelësit privat të një çifti çelësash asimetrikë ose një çelësi të njohur bashkërisht nga palët që përdorin çifte çelësash simetrikë.
Proxy	Agjent që pranon kërkesat nga klientët dhe më pas krijon lidhje me klientët e tjerë nga adresa e tij IP.
Server	Program brenda konceptit klient-server ose kompjuter në të cilin funksionon ky program.

Program përgjimi	Kryesisht programe trojane që mbledhin informacione rreth aktiviteteve të përdoruesit dhe ua përcjellin ato palëve të treta.
Shifrim simetrik	Një çelës i vetëm përdoret si për shifrim ashtu edhe për deshifrim.
TAN	Lidhet me mTAN, eTAN, iTAN - Numri i vërtetimit të transaksionit - fjalëkalim që përdoret vetëm një herë në veprimet bankare online.
Trojan	(Kalë Troje) Kombinimi i një programi mbartës me një pjesë të fshehtë me qëllim të keq, shpesh program përgjimi ose derë e pasme. Një kalë Troje nuk përhapet vetvetiu, por nxit përdoruesin ta instalojë atë duke reklamuar dobinë e programit mbartës.
Trolling	Shihni Ngacmimet Online
VOIP	Protokolli i Zërit Përmes Internetit - Telefonia përmes Internetit - Të dhënat e të folurit digjitalizohen dhe dërgohen përmes Internetit në paketa të vogla të dhënash.
VPN	Një rrjet privat virtual shtrin në mënyrë të sigurt një rrjet privat në një rrjet publik, siç është Interneti.

SHKURTESA	
AfriNIC	Qendra Afrikane e Informacionit për Rrjetat
API	Një ndërfaqe programimi për aplikacione
APNIC	Qendra e Informacionit për Rrjetat në Azi dhe Paqësor
ARIN	Regjistri Amerikan për Numrat e Internetit
ARP	Protokolli i Zgjidhjes së Adresave
ASN	Numër Sistemi Autonom
ASN.1	Shënim Abstrakt Sintakse Një
Partnerët e AV	Partnerët e antiviruseve
BIA	Adresa e salduar (lidhet me MAC)
C&C	Komandim dhe Kontroll
CCIU	Njësia e Hetimeve të Krimeve Kompjuterike
CHIS	Burim i Fshehtë Zbulimi Njerëzor
CSP	Operator i Shërbimeve të Komunikimit
DBPN	Drejtoria e Bashkëpunimit Policor Ndërkombëtar, Tiranë
DDoS	Bllokim i Shpërndarë i Shërbimeve
DFU	Njësia e Forensikës Digjitale
DNS	Server Emrash Domenes (Domain Name Server)
DNS	Sistemi i Emrave të Domeneve përkthen domene ose adresa faqesh në adresa IP
DoS	Bllokim i Shërbimeve
DPR	Kërkesë për Ruajtje të Dhënash
Drop	Shpërndarës
KEDNj	Konventa Evropiane për të Drejtat e Njeriut
Eurojust	Rrjeti Gjyqësor Evropian
Europol	Agjencia Policore Evropiane

FCU	Njësia e Krimit Financiar
FTP	Protokolli i Transferimit të Skedarëve
HTTP	Protokolli i Transferimit të Hipertekstit
HTTPS	Protokolli i Sigurt i Transferimit të Hipertekstit
IANA	Autoriteti i Numrave të Alokuar në Internet
ICPO	Organizata Ndërkombëtare e Policisë Penale (Interpol)
IDN	Emër domeni i ndërkombëtarizuar
IDNA	Ndërkombëtarizimi i Emrave të Domeneve në Aplikacione
IMAP	Protokolli i Qasjes së Mesazheve në Internet
IMEI	Identiteti ndërkombëtar i pajisjes celulare
IMSI	Identiteti ndërkombëtar i pajtimtarit celular
IP	Protokolli i Internetit
IP	Adresë e Protokollit të Internetit
IP Address	Adresë e Protokollit të Internetit
IPv4	Adresë e Protokollit të Internetit, Versioni 4
IPv6	Adresë e Protokollit të Internetit, Versioni 6
ISP	Operator i Shërbimit të Internetit
JIT	Ekip i Përbashkët Hetimor
KPP	Kodi i Procedurës Penale i Republikës së Shqipërisë
LACNIC	Qendra e Informacionit për Rrjetat e Amerikës Latine dhe Karaibeve
LAN	Rrjet lokal
LEGAT	Atashetë ligjorë të FBI në ambasadat e SHBA
MAC	Kontrolli i Qasjes së Medias
MiM	Sulm me Ndërhyrës të Ndërmjetëm

MIM	Sulm me Ndërhyrës të Ndërmjetëm
MITM	Sulm me Ndërhyrës të Ndërmjetëm
MitM	Sulm me Ndërhyrës të Ndërmjetëm
MLAT	Traktati i Ndihmës Ligjore Reciproke
MX	Server për Email
NCB	Byroja Qendrore Kombëtare, Njësi e Interpolit
NIC	Kartë ndërfaqeje rrjeti
ns	Simulues rrjeti (veçanërisht ns-1, ns-2 dhe ns-3).
OLAF	Zyra Evropiane e Luftës Kundër Mashtrimeve
OSINT	Zbulimi i të Dhënave nga Burime të Hapura
P2P	Peer-to-Peer
P2P	Peer-to-Peer
POP3	Protokolli i Postës 3
Prokuroria	Zyra e Prokurorisë
RIPE	Rrjetat IP Evropiane (Qendra e Informacionit për Rrjetat në Evropë)
RIR	Regjistrues Rajonal i Internetit
SaaS	Softueri si Shërbim
SELEC	South East Law Enforcement Center
SIM	Moduli i Identitetit të Pajtimtarit
SMTP	Protokolli i Thjeshtë i Transferimit të Postës
SSH	Secure Shell
TAN	Numri i Autentikimit të Transaksionit
TCP	Protokolli i Kontrollit të Transmetimeve
TCP/IP	Protokolli i Kontrollit të Transmetimeve / Protokolli i Internetit
Telnet	Protokoll i Shtresës së Aplikacioneve
TLS	Siguria e Shtresës së Transportit

VOIP	Zëri Përmes Protokollit të Internetit
VOIP	Zëri Përmes IP
VPN	Rrjet privat virtual
WAN	Rrjet i Hapësirave të Gjera
Wi-Fi	Rrjet pa tela (me valë)
WLAN	Wireless Local Area Network
WWW	World Wide Web www.

SHTOJCA

Udhëzimi për Hetimet e mbështetura mbi Burime të Hapura (shtojca 1)

Kërkesa për Ndihmë Juridike të Ndërsjelltë për të dhënat e pajtimtarit (shtojca 2)

Kërkesa për Ruajtjen e të Dhënave (shtojca 3)

SHTOJCA 1

Udhëzimi për Hetimet e mbështetura mbi Burime të Hapura

PARALAJMËRIM: *Çdo kërkim dhe hetim online lë gjurmë. Prandaj, do të duhet të merret një vendim operacional nëse dëshironi të siguroheni që kërkimi juaj është i pa-atribueshëm, pra nuk mund të gjurmohet tek organet e zbatimit të ligjit ose tek individët e identifikueshëm, apo nëse dëshironi që ai të mund të atribuohet, pra të gjurmohet, tek forcat e rendit.*

1. Përcaktoni dhe vendosni "çështjet për të provuar" të hetimit dhe se çfarë të dhënash janë mbledhur tashmë.

2. Hartoni një profil komunikimi dhe vendosni parametrat e hetimit.

3. Zgjidhni pajisjet dhe mjetet më të përshtatshme për hetimin.

4. Bini dakord për metodologjinë dhe formatin e emërtimeve për ruajtjen e materialeve në dosje për lehtësi në referim, shqyrtim dhe/ose dorëzim.

5. Kur kërkoni për emra dhe numra, merrni parasysh çdo ndërtim të mundshëm, duke përfshirë pseudonimet, emrat e përdoruesve, emrat e llogarive, kodet e prefikseve, formatin etj.

6. Sigurojeni menjëherë materialin që përbën interes duke përdorur programe për kopjim ekrani apo shtojca për shfletuesit.

7. Mbani parasysh mundësinë që të përdorni programe për kopjimin e ekranit me qëllim që të ruani të gjithë hetimin që po zhvillohet online.

8. Përdorni teknika të përparuara kërkimi dhe merrni parasysh indekset dhe domenet rajonale.

9. Kërkoni në baza të dhënash të tilla si regjistri zgjedhor, numëratorët telefonikë, baza të dhënash tregtare, harta, si dhe faqe për gjenealogjitë.

10. Kërkoni në faqe rrjetesh sociale dhe komunitetesh online si Facebook, Twitter dhe Instagram për emra, adresa e-mail dhe numra telefoni.

11. Kërkoni në faqe për shitblerje, grupe dhe mbajtje kodi.

12. Kërkoni për objektiva dytësore si miqtë, bashkëpunëtorët, pjesëtarët e familjes, ish-partnerët, fëmijët etj. (Hije Digjitale).

13. Kërkoni për informacion periferik si mjete automobilistike, adresa të mëparshme, imazhe apo informacion në shtyp që u referohen veprave penale të ngjashme apo të së shkuarës.

14. Kërkoni në faqe që merren me media vizuale, të tilla si as Google Images, Flickr, YouTube, Tin eye etj.

15. Përcaktoni emrat e subjekteve regjistrues dhe mbajtësit e tanishëm dhe historikë të adresave IP apo domeneve.

16. Përdorni mjete përkthimi për të kërkuar për informacion në gjuhë të tjera.

17. Ekzaminoni imazhet digjitale për informacion shtesë dhe eksploroni të dhënat EXIF për datën, orën, specifikimin e pajisjes krijuese dhe vendndodhjen fizike.

18. Ndiqni kokat e e-mail deri në pikën e origjinës dhe mblidhni informacion për rrjetet / pajisjet.

19. Mbani regjistër auditimi, si për metodologjinë tuaj të mbledhjes së të dhënave, ashtu edhe për provat e gjetura, pasi në këtë fazë ato do të përbëjnë prova kërkimi dhe prokuroria do të ketë nevojë të përsërisë metodologjinë për të përftuar të njëjtat rezultate dhe për t'i paraqitur si prova në gjykatë.

20. Kini parasysh nenin e KPP për masat e posaçme hetimore – autorizimet që kërkohen nga prokuroria.

SHTOJCA 2

Miratuar nga T-CY në Seancën e saj të 19-të Plenare

T-CY(2018)10

Strasburg, 9 korrik 2018

[Shtoni logon ose përdorni kokën që përdor zakonisht institucioni në dokumente nëse është e nevojshme]

Kërkesë për Ndihmë të Ndërsjellë Juridike për informacion në lidhje me pajtimtarë të caktuar

sipas nenit 31 të Konventës së Budapestit për Krimin Kibernetik[1]

datë
DD/MM/VVVV

❒ numri i referencës / numri i çështjes

statusi i kërkesës
❒ Vazhdim i një kërkese të mëparshme MLA (detajet më poshtë)
❒ Vazhdim i një kërkese të mëparshme për ruajtje të dhënash (detajet më poshtë)

AUTORITETI TË CILIT I DREJTOHET KËRKESA

Autoriteti KËRKUES	
Organizata/Institucioni	
Personi përgjegjës për kërkesën	
Adresa	
Numri i telefonit	

1 Ky formular/model është miratuar nga Komiteti i Konventës për Krimin Kibernetik (T-CY) në Sesionin e tij të 19[të] Plenar (9-10 korrik 2018) për të lehtësuar përgatitjen dhe pranimin e kërkesave nga ana e palëve. Përdorimi i këtij modeli nga Palët e Konventës së Budapestit është fakultativ.

Numri i celularit	
Adresa e email-it	
Numri i faksit	
Orari zyrtar	
Zona kohore	
❒	Preferohet përgjigje me email ose mjete të tjera të përshpejtuara
❒	Preferohet përgjigja me anë të:

NËSE nevojitet konfirmim SHTESË NGA autoriteti kërkues, JU LUTEMI KONTAKTONI:	
Emri:	
Titulli i pozicionit:	
Funksioni:	
Numri i telefonit	
Numri i celularit	
Adresa e email-it	

AUTORITETI hetues/operativ i ngarkuar me çështjen **(nëse është i ndryshëm nga Autoriteti Kërkues)**	
Organizata/Institucioni	
Personi përgjegjës i çështjes	
Adresa	
Numri i telefonit	
Numri i celularit	
Adresa e email-it	
Numri i faksit	

Prokuroria ose gjykata përgjegjëse, sipas rastit	
Prokuroria përgjegjëse dhe numri i çështjes	
Gjykata përgjegjëse dhe numri i çështjes	
Vendimet e prokurorisë apo gjykatës lidhur me kërkesën për MLA	

Informacion për një kërkesë të mëparshme për MLA nëse ka	
Datë	
Numri i biletës/referencës	
Detaje kontakti të autoritetit që ka kërkuar një MLA më parë	
Detaje kontakti të autoritetit që i janë përgjigjur (ose që e kanë ekzekutuar) MLA-në e mëparshme	
Mënyra e komunikimit e përdorur për paraqitjen e kërkesës së mëparshme (adresa e emailit, numri i faksit, etj.)	

Informacion për ruajtje të mëparshme të dhënash Sipas kërkesës Nëse ka	
Datë	
Numri i biletës/referencës	
Detajet e kontaktit të autoritetit që ka kërkuar ruajtjen e të dhënave	
Detajet e kontaktit të autoritetit që i është përgjigjur (ose që ka ekzekutuar) kërkesën për ruajtje të dhënash	
Kanali i komunikimit	

Baza ligjore vendase për kërkesën NËSE KA	
Vendimi përkatës nga Gjykata, Prokuroria apo nga organi tjetër i autorizuar; ose baza tjetër ligjore për kërkesën Ju lutemi, bashkëngjitni urdhrin ose autorizimin statutor	

përmbledhje e çështjes Duke përfshirë: - përshkrim i shkurtër i fakteve - si lidhen të dhënat e kërkuara me hetimin/veprat penale - qëllimi dhe domosdoshmëria e kërkesës për zbulim informacionesh mbi abonentët - akuzat e ngritura/lista e veprave penale (duke iu referuar dispozitave ligjore vendase dhe penaliteteve në fuqi)

STATUSI I ÇËSHTJES
❒ Në fazë gjykimi Detaje të tjera:

INFORMACIONET E PAJTIMTARËVE që kërkohen të nxirren[2]		
Informacioni i abonentit në lidhje me adresat e mëposhtme IP që kërkohet:		
Informacioni për abonentin në lidhje me llogaritë e mëposhtme:		
Periudha me interes	Data e fillimit: DD/MM/VVVV Ora e fillimit (dhe zona kohore):	Data e përfundimit: DD/MM/VVVV Ora e përfundimit (dhe zona kohore):

2 Përdor SHTOJCËN për detaje.

Informacion që identifikon ofruesin e shërbimit DHE – nëse ka – vendndodhjen e sistemit kompjuterik

Ju lutemi, jepni sa më shumë informacion që të jetë e mundur për të ndihmuar në identifikimin e ofruesit të shërbimit (duke përfshirë pseudonimet, numrat e telefonit dhe detaje të tjera kontakti ose adresa emaili të lidhura me to)

SHKALLA E URGJENCËS

URGJENTE

Përgjigja pritet nga: DD/MM/VVVV

ARSYET E URGJENCËS (shënoni më shumë se një arsye, nëse janë disa)

❒ Kërcënim për humbje jete ose për plagosje të rëndë

❒ I dyshuari/autori në arrest me burg

❒ I dyshuari/autori pritet të lirohet nga paraburgimi

❒ Vepra penale në proces e sipër

❒ Ndryshimet e shpejta të të dhënave

❒ Kërcënim i menjëhershëm i një natyre serioze për sigurinë publike

❒ Skadimi i afatit të parashkrimit

❒ Ka filluar ose pritet të fillojë shumë shpejt gjyqi.

❒ Tjetër:

Detaje të shkurtra për urgjencën

KONFIDENCIALITETI

❒ Kërkojmë që kjo kërkesë të mbahet konfidenciale dhe klientët të mos njoftohen. Ju lutemi na informoni nëse ligji juaj i brendshëm kërkon që ne të shpjegojmë arsyen e konfidencialitetit; ose – përpara se të ndërmerrni ndonjë veprim – nëse ligji juaj vendas kërkon njoftimin e klientit ose nëse dyshoni se ofruesi mund të mos e përmbushë kërkesën për ruajtjen e konfidencialitetit.

Kërkohet konfirmim/njoftim

❒ Konfirmimi i marrjes së kërkesës

❒ Nëse nevojitet ndonjë informacion tjetër dhe çfarë informacioni nevojitet nga shteti kërkues për të ekzekutuar kërkesën

❒ Informacion mbi disponueshmërinë e të dhënave ose nëse të dhënat janë jashtë juridiksionit të vendit të kërkuar

❒ Tjetër:

SHËNIME shtesë, NËSE KA

Nënshkrimi dhe/ose vula e autoritetit KËRKUES nëse është e aplikueshme

Emri	
Pozicioni	

Data / vendi	
Nënshkrimi dhe/ose vula	

21 Shtojca: Detajet e informacionit të kërkuar[3]

Informacioni i abonentit që duhet për adresat IP		
Informacioni i abonentit në lidhje me adresën/adresat IP të kërkuara (në masën e lejuar nga ligji juaj):		
Periudha me interes:	Data dhe ora e fillimit:	Data dhe ora e përfundimit:
Zona kohore:		
Detajet e kërkuara:		

☐	Emrat e abonentëve	
☐	Emrat e përdoruesve	
☐	Emrat e ekranit, ose identitete të tjera	
☐	Email, media sociale dhe llogari të tjera që lidhen me adresën/at IP	
☐	Adresat postare	
☐	Adresat e banimit	
☐	Adresat e biznesit	

3 Ju lutemi, vini re se ligji i shtetit të kërkuar mund të mos i konsiderojë domosdoshmërisht të gjitha të dhënat e mëposhtme si informacione të pajtimtarëve.

☐	Numrat e telefonit, informacione të tjera kontakti	
☐	Të dhënat e faturimit	
☐	Adresa e faturimit	
☐	Metoda e pagesës	
☐	Historiku i Pagesave	
☐	Periudha e faturimit	
☐	Informacion në lidhje me kohëzgjatjen e shërbimit dhe llojet e shërbimeve që kanë përdorur abonentët ose klientët	
☐	Çdo informacion tjetër identifikues, pavarësisht nëse këto të dhëna janë në formë elektronike ose në forma të tjera	

Informacioni i abonentit që nevojitet për llogaritë		
Informacion mbi llogaritë/llogaritë e mëposhtme të kërkuara, në masën e lejuar nga ligji juaj:		
Periudha me interes:	Data dhe ora e fillimit:	Data dhe ora e përfundimit:
Zona kohore:		
Detajet e kërkuara:		

☐	Emrat e abonentëve	
☐	Emrat e përdoruesve	
☐	Emrat e ekranit, ose identitete të tjera	
☐	Adresat postare	
☐	Adresat e banimit	
☐	Adresat e biznesit	
☐	Adresat e emailit	

☐	Numrat e telefonit, informacione të tjera kontakti	
☐	Të dhënat e faturimit	
☐	Adresa e faturimit	
☐	Metoda e pagesës	
☐	Historiku i Pagesave	
☐	Periudha e faturimit	
☐	Data e regjistrimit	
☐	Adresa IP e përdorur për regjistrimin fillestar të llogarive	
☐	Data e fundit e regjistrimit të aksesit	
☐	Adresa IP e përdorur për aksesin e fundit të regjistruar në llogari	
☐	Adresa IP e përdorur për të hyrë në llogari në periudhën: Data e fillimit: DD/MM/VVVV Ora: Data e përfundimit: DD/MM/VVVV Ora: Zona kohore:	
☐	Emaile të tjera, media sociale dhe llogari të tjera që lidhen me personin ose llogarinë	
☐	Informacion në lidhje me kohëzgjatjen e shërbimit dhe llojet e shërbimeve që kanë përdorur abonentët ose klientët	
☐	Çdo informacion tjetër identifikues, pavarësisht nëse këto të dhëna janë në formë elektronike ose në forma të tjera	

SHTOJCA 3

Miratuar nga T-CY në Seancën e saj të 19-të T-CY(2018)11

Strasburg, 9 korrik 2018

[Shtoni logon ose përdorni kokën që përdor zakonisht institucioni në dokumente nëse është e nevojshme]

Kërkesë për Ruajtjen e të Dhënave sipas neneve 29 dhe 30 të Konventës së Budapestit për krimin kibernetik[4]

datë
DD/MM/VVVV

numri i referencës / numri i çështjes

STATUSI I KËRKESËS
❒ Kërkesë e re
❒ Zgjatje e kërkesës së mëparshme
❒ Numri i biletës/referencës së kërkesës së mëparshme:

AUTORITETI TË CILIT I DREJTOHET KËRKESA

Autoriteti KËRKUES *	
Organizata/Institucioni	
Personi përgjegjës për kërkesën	

4 Ky formular/model është miratuar nga Komiteti i Konventës për Krimin Kibernetik (T-CY) në Sesionin e tij të 19tw Plenar (9-10 korrik 2018) për të lehtësuar përgatitjen dhe pranimin e kërkesave nga ana e palëve. Përdorimi i këtij modeli nga Palët e Konventës së Budapestit është fakultativ. Ju lutemi vini re se zërat e shënuar me yll (*) janë informacion i kërkuar në përputhje me nenin 29, paragrafi 2 i Konventës për krimin kibernetik.

Adresa	
Numri i telefonit	
Numri i celularit	
Adresa e email-it	
Numri i faksit	
Orari zyrtar	
Zona kohore	
	Preferohet përgjigje me email ose mjete të tjera të përshpejtuara
	Preferohet përgjigja me anë të:

NËSE nevojitet konfirmim SHTESË NGA autoriteti kërkues, JU LUTEMI KONTAKTONI:	
Emri:	
Titulli i pozicionit:	
Funksioni:	
Numri i telefonit	
Numri i celularit	
Adresa e e-mailit	

AUTORITETI hetues/operativ i ngarkuar me çështjen **(nëse është i ndryshëm nga autoriteti kërkues)**	
Organizata/Institucioni	
Personi përgjegjës në autoritet	
Adresa	
Numri i telefonit	
Numri i celularit	
Adresa e e-mailit	
Numri i faksit	

Prokuroria ose gjykata përgjegjëse nëse ka	
Prokuroria përgjegjëse dhe numri i çështjes	
Gjykata përgjegjëse dhe numri i çështjes	
Vendimet e prokurorisë apo gjykatës lidhur me kërkesën	

NDJEKJE PËRMES NDIHMËS JURIDIKE RECIPROKE	
❒	Ju informojmë se kemi në plan t'ju paraqesim një kërkesë për ndihmë të ndërsjellë juridike për t'ju kërkuar që të na ofroni disa të dhëna. *
❒	Ju lutemi gjeni bashkangjitur një kërkesë për ndihmë të ndërsjellë juridike për ofrimin e disa të dhënave.

VEPRAT PENALE OBJEKT I HETIMIT APO PROCEDIMIT PENAL *	
❒ Veprat penale që korrespondojnë me nenet 2 deri në 11 të Konventës së Budapestit	Ju lutemi, specifikoni veprat penale sipas ligjit të Shtetit kërkues:
❒Vepra/vepra të tjera penale	Ju lutemi, specifikoni sipas ligjit të Shtetit kërkues:

Përmbledhje e çështjes *

Duke përfshirë:

- një përshkrim të shkurtër të fakteve

- si lidhen të dhënat e kërkuara me hetimin/veprat penale

- qëllimi dhe domosdoshmëria e kërkesës për ruajtjen dhe/ose zbulimin e pjesshëm të të dhënave të trafikut

- akuzat e ngritura/lista e veprave penale në këtë çështje

Të dhënat që duhen ruajtur*	
❒ **Informacioni i abonentit**	Ju lutemi, specifikoni:
Periudha e interesit	Data e fillimit: DD/MM/VVVV Data e përfundimit: DD/MM/VVV Koha (dhe zona kohore): Koha (dhe zona kohore):
❒ Nëse sistemi është një sistem i përbashkët, ju lutemi ruani të gjitha informacionet bazë të abonentëve për të gjitha sistemet virtuale në IP.	
❒ **Të dhënat e trafikut**	Ju lutemi, specifikoni:
Periudha e interesit	Data e fillimit: DD/MM/VVVV Data e përfundimit: DD/MM/VVVV Koha (dhe zona kohore): Koha (dhe zona kohore):
❒ **Të dhënat e përmbajtjes**	Ju lutemi, specifikoni:
Periudha e interesit	Data e fillimit: DD/MM/VVVV Data e përfundimit: DD/MM/VVVV Koha (dhe zona kohore Koha (dhe zona kohore):

Informacion që identifikon personin ose organizatën (p.sh. OPERATORIN e shërbimit) që ka në posedim ose që kontrollon të dhënat kompjuterike të ruajtura DHE vendndodhjen e sistemit kompjuterik, NËSE KA *

KONFIDENCIALITETI

❒ Kërkojmë që kjo kërkesë të mbahet konfidenciale dhe të mos njoftohen klientët.

Ju lutemi na informoni nëse ligji juaj i brendshëm kërkon që ne të shpjegojmë arsyen e konfidencialitetit; ose – përpara se të ndërmerrni ndonjë veprim – nëse ligji juaj vendas kërkon njoftimin e klientit ose nëse dyshoni se ofruesi mund të mos e përmbushë kërkesën për ruajtjen e konfidencialitetit.

SHËNIME SHTESË, NËSE KA

Nënshkrimi dhe/ose vula e autoritetit kërkues nëse ka

Emri	
Pozicioni	
Data / vendi	
Nënshkrimi dhe/ose vula	

Shtojca: Formulari i specifikimit të të dhënave

Ju lutemi, plotësoni një formular më vete për çdo person ose organizatë që besohet se zotëron ose kontrollon të dhënat. Ju lutemi, plotësoni sa më shumë të dhëna që është e mundur ose sa më shumë që të ketë.

Detajet e personit ose organizatës që besohet se zotëron ose që ka nën kontroll të dhënat

Emri i biznesit		
Emri ligjor		
Emri i kontaktit		
Adresa		
Vendi/Shteti		
Telefoni		

Email		
Adresa		
IPv4	**1-255**	**1-255**
URL		
Data		
Ora		
Brezi orar		
Proxy		
Anonimizimi		
Numri i portës		
IPv6	**Subnet – 64 bit**	**Host – 64 bit**
URL:		
Data		
Ora		
Zona kohore		
Proxy		
Anonimizimi		
Të dhëna të tjera		
Adresa e e-mailit		
ID e rrjeteve sociale		
Data		
Ora		
Zona kohore		
Proxy		
Anonimizimi		