

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Aleksandr Drozdov 179697IAAB

TALTECHI TEADMISTE VÕTI - ÜLIKOOLI DIGITAALNE VISIITKAART

Bakalaureusetöö

Juhendaja: Edmund Laugasson
MSc

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Aleksandr Drozdov

29.04.2021

Annotatsioon

Käesoleva bakalaureusetöö eesmärk on luua eeldus Tehnikaülikooli digitaalse visiitkaardi loomiseks.

Lõputöö käigus kirjutas autor skripti ISO-faili loomiseks ja kirjeldas meetodi mä lupulga ehk digitaalse visiitkaardi komponendi ettevalmistamiseks.

Väljatöötatud skript muudab Linux Minti vastavalt TalTechi nõuetele. See muudetud distributsioon on kõrgendatud privaatsusega ja turvalisusega. Selle skripti toimimisjärjekord on selline – vaikumisi ISO-faili lahti pakkimine, selle ISO-faili muutmine, sulgemine ja uue ISO-faili, kontrollsummade loomine.

Käesoleva töö tulemusena loodi eeldus edasiarenduseks – kirjutati skript, töötati välja skript mä lupulgale paigaldava ISO valmistamiseks, loodi juhend.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 49 leheküljel, 12 peatükki, 14 joonist, 5 tabelit.

Abstract

THE KEY TO TALTECH'S KNOWLEDGE - THE UNIVERSITY DIGITAL VISIT CARD

The aim of this bachelor's thesis is to create a precondition for creating a digital business card of the Technical University.

During the thesis, the author wrote a script to create an ISO file and described a method for preparing an USB memory stick for digital business card component.

The developed script modifies the Linux Mint according to the requirements of TalTech. This modified distribution is enhanced with privacy and security. The logic of this script is to decompress the default ISO file, modify it, close, and create checksums and the new ISO file.

As a result of this work, a precondition for further processing was created - a script was written, a method for making an ISO-file was developed, and a manual was created.

The thesis is in 49 and contains 12 pages of text, 12 chapters, 14 figures, 5 tables.

Lühendite ja mõistete sõnastik

DPI	<i>Dots per inch</i> , punkti tolli kohta
IA	Arvutisüsteemide instituut
OS/OP	Operatsioonisüsteem
ISO-fail	<i>Disc Image</i> , tõmmisfail, mis on täieliku kujutisega kogu CD, DVD või BD andmekandjast, vastavalt ISO 9660 standardile
USB	<i>Universal Serial Bus</i> , liides välisseadmete arvutiga ühendamiseks
BIOS	<i>Basic Input/Output System</i> , baasvahetussüsteem
UEFI	<i>Unified Extensible Firmware Interface</i> , Laiendatav püsivara liides
RAM	<i>Random Access Memory</i> , muutmälu
SSD	<i>Solid State Drive</i> , pooljuhtketas
HDD	<i>Hard Disk Drive</i> , kõvaketas
GUI	<i>Graphical User Interface</i> , graafiline kasutajaliides

Sisukord

Autorideklaratsioon	2
Annotatsioon.....	3
Abstract.....	4
Lühendite ja mõistete sõnastik	5
Sisukord.....	6
Tabelite loetelu	9
Tabelite loetelu	10
1 Sissejuhatus	11
1.1 Probleem.....	11
1.2 Eesmärk	11
1.3 Metodoloogia.....	12
2 Sihtrühm ja piirangused.....	13
2.1 Sihtrühm	13
2.2 Piirangud.....	13
3 Võrdlus	14
3.1 Esimene etapp.....	14
3.1.1 Turuosa	14
3.1.2 Tuum.....	15
3.1.3 Süsteeminõuded.....	15
3.1.4 Esimene etappi kokkuvõtte.....	16
3.2 Teine etapp	17
3.2.1 Turvalisus	17
3.2.2 Privaatsus.....	19
3.2.3 MS Windows	19
3.2.4 macOS	20
3.3 Võrdluse kokkuvõtte.....	20
4 Linuxi privaatsed distributiivid	21
4.1 Tails	21

4.2 Linux Kodachi	22
4.3 Septor.....	23
4.4 Etic hack süsteemid	23
4.5 Kokkuvõtte	23
5 Nõuded privaatsusele ja turvalisusele.....	25
5.1 Vabavaraligus.....	25
5.2 Kaitstud veebilehitsejad.....	25
5.3 <i>Incognito</i> režiim.....	26
5.4 Privaatne otsingumootor.....	26
5.5 Lõikepuhvri kustutamine	26
5.6 Tehtavad tegevused ei salvestu.....	26
6 Linux Mint.....	27
7 Tingimused	28
8 Tulemused	30
8.1 Koodi jagamine.....	30
8.2 Skripti kirjeldus	30
8.2.1 ISO ühendamise ja lahti pakkimise	31
8.2.2 Skript moodulite ja DNS-serveri ühendamiseks	32
8.2.3 Skript süsteemi konfigureerimiseks ja muutmiseks	32
8.2.4 ID-kaardi tarkvara paigaldamine	32
8.2.5 Veebilehitseja Brave.....	33
8.2.6 <i>Incognito mode</i> vaikimisi	33
8.2.7 Lõikepuhvri kustutamine.....	33
8.2.8 Teised asjad	33
8.2.9 Puhastamine.....	33
8.2.10 Skript <i>chroot</i> 'ist väljumiseks.....	34
8.2.11 <i>Chroot</i> 'i käivitamine	34
8.2.12 ISO loomine.....	34
8.3 Mälupulga valmistamise meetod	36
8.3.1 Ventoy välimuse muutmine.....	36
8.4 Juhendi loomine.....	37
9 Analüüs.....	38
9.1 Tulemuste analüüs	38
9.2 Lähtetingimuste analüüs	40

10 Tulevikuarendused.....	41
12 Kokkuvõte	42
Kasutatud kirjandus	43
Lisad	45
Lisa 1. Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks	45
Lisa 2. Skripti kood	46

Tabelite loetelu

Tabel 1. Operatsiooni süsteemide populaarsus <i>Netmarketshare</i> järgi.....	15
Tabel 2. OSide miinimum süsteeminõuded.....	16
Tabel 3. Süsteemide võrdlus.....	17
Tabel 4. OSide erinevused turvalisuses	18
Tabel 5. Distributiivide võrdlev tabel.....	24

Tabelite loetelu

Joonis 1 Skripti visuaalne vaade.....	31
Joonis 2. Ventoy välimus	37
Joonis 3. Juhend eesti keeles	37
Joonis 4. Paigaldused ja lahti pakkimine.....	46
Joonis 5. <i>Chroot</i> 'i ettevalmistamine.....	46
Joonis 6. ISO muutused – ID-kaardi tarkvara, Brave veebilehitseja.....	47
Joonis 7. ISO muutused – tundmatu režiim vaikimisi, löikepuhvri kustutamine.....	47
Joonis 8. ISO muutused - taustapilt ja puhastamine.....	47
Joonis 9. <i>Chroot</i> 'i käivitamine	47
Joonis 10. Manifest faili muutus	48
Joonis 11. Vana failisüsteemi kustutamine ja uue failisüsteemi pakkimine.....	48
Joonis 12. Uue ISO-faili ja kontrollsumma loomine.....	48
Joonis 13. Puhastamine	48
Joonis 14. Modifitseeritud OSi töölaud.....	49

1 Sissejuhatus

„Property must be secured, or liberty cannot exist.” – John Adams [1].

Kahekümne esimesel sajandil on meie kohta käivad andmed muutunud meie omandiks ja puutumatus vajavaks tooteks. Kui seda põhimõtet saab reaalses elus enam-vähem jälgida, siis virtuaalses ruumis üritatakse väga sageli tungida meie kohta käivatesse andmetesse.

Tänapäeval pole enamikus arvutites ja serverites kasutatavad operatsioonisüsteemid kahjuks piisavalt privaatsed, turvalised ja konfidentsiaalsed. Kavatsen oma töö alguses kinnitada seda väikese uuringuga, mis näitab selgelt, kuidas ja miks neid süsteeme ei eelistada tundlike või privaatsete andmetega töötamisel, nagu internetipank, terviseandmete vaatamine, äri, tehingud krüptorahakottidega.

Enne töö kirjutama asumist toimus ülikooli avalike suhete osakonnaga kohtumine, mille käigus selgus, et ülikool vajab toodet, mis esindaks asutust kui Eesti juhtivat tehnoloogiaasutust. Otsustati seda teha.

1.1 Probleem

Töö käigus pean looma prototüübi, mis lahendab kolm probleemi.

- Tehnikaülikooli kui tehnikaalast kõrgharidust andva ülikooli tutvustamine tehniliselt funktsionaalse ja innovaatilise lahenduse abil ja Eesti tehnikavaldkonna pioneeri rolli esiletoomine.
- Turvaline, privaatne, kiire lahendus tundlike teenuste kasutamiseks (internetipank, terviseandmed, ettevõtte ärisaladused).
- Andmete päästmine mittetöötava operatsioonisüsteemiga arvutist. Samuti arvuti kasutamise võimaldamine sisemise andmekandja rikke korral.

1.2 Eesmärk

Bakalaureusetöö eesmärk on luua eeldus Tehnikaülikooli digitaalse visiitkaardi loomiseks. Selleks on vaja luua skript ISO-faili prototüübi loomiseks, OSiga ühes

paljust GNU/Linux'i distributsioonidest. See distributsioon peab vastama lähtetingimustele, näiteks on võimalik teostada tööd ID-kaardiga jne.

Loodud ISO-fail on ka ülikooli komplekti edasiarendamise eeltingimus. See komplekt võib sisaldada: TalTech'i kujundusega karpi, käesolevas töös loodud ISO-failiga USB-mälupulka, võib olla HSM-moodulit, miniatuurne ID-kaardi lugeja. See kõik kokku on Tallinna Tehnikaülikooli digitaalne visiitkaart. Samuti käesoleva töö võiks kasutada dokumentatsiooniks edasiarendamises.

1.3 Metodoloogia

Töö teoreetilises osas viiakse läbi uuring populaarsete operatsioonisüsteemide kohta, analüüsitakse olemasolevaid operatsioonisüsteeme ja nende distributsioonid ning vastavalt nõutavatele tingimustele ja ülesannetele valitakse sobiv. Seejärel kirjeldatakse tingimused ja piirangud.

Praktilise osas valitakse üks konkreetne tingimustele vastav operatsioonisüsteem, mille näitel luuakse ISO-faili prototüüp vastavalt tingimustele. Lisaks sellele luuakse ISO-faili kontrollsumma allalaadimisel terviklikkuse kontrolliks. Kirjutakse ka juhend ISO-faili USB-pulgale kirjutamiseks ja dokumenteeritakse tegevused veebipõhiselt, et ülikoolil oleks võimalik seda kasutusele võtta ja edasi arendada. Ja viimasena luuakse ISO-faili loomise skript, mis uuendab ära OSi ja rakendab kõrgendatud turvalisuse ja privaatsuse sätteid.

2 Sihtrühm ja piirangused

2.1 Sihtrühm

Pärast kohtumist TalTechi PR-osakonnaga otsustati määrata selle projekti sihtgrupiks järgmised kasutajad:

- isikud, kellel pole kogemusi GNU/Linuxil ja selle distributsioonidel põhinevate operatsioonisüsteemidega
- kooli lõpetajad
- Windowsi kasutajad
- erinevate olümpiaadide osalejad
- TalTechi astujad

2.2 Piirangud

Siiski on mõned piirangud. Siis (OSis) peab olema võimalus töötada ID-kaarditarkvaraga ja teostada kõik operatsioonid sellega, eks siis dokumentide allkirjastamine, dokumentide vaatamine, ID-kaardiga sisselogimine ja failide krüpteerimine.

Järgmine piirang on selline, et OS peab kasutab võimalikult vähe riistvararessurssi. See on eeldus selleks, et vähendada erinevate protsesside ja tarkvarade kogum OSis.

Ja viimane piirang – ligipääsetavus sihtrühmale. Kujundus, välimus ja funktsionaalsus peab olema aru saadav algajatele ja inimesele, kes GNU/Linuxit palju ei kasutanud.

3 Võrdlus

Esimene asi, mida käesolevas töös tuleb teha, on võrrelda kõige populaarsemaid arvuti OSi, et valida projekti jaoks sobiv. Võrdlus toimub kahes etapis. Esimene on süsteemide üldine võrdlus selliste parameetrite osas nagu riistvaranõuded, töö kiirus, populaarsus jne. Teises etapis võrreldakse turvalisust ja konfidentsiaalsust.

Portaali *Netmarketshare* [2] andmetele tuginedes on laua- ja sülearvutites kõige populaarsemad operatsioonisüsteemid MS Windows, macOS ja Linux. Seda võib näha alltoodud tabelist, andmed, mis võeti samast portaalist.

3.1 Esimene etapp

Esimeses etapis tuleb võrrelda loetletud operatsioonisüsteemide põhiomadusi. Need omadused on - toetatud arvuti arhitektuurid, sihtsegment, litsentsi tüüp ja tuumad jne.

Microsofti välja töötatud patenteeritud OSide perekond. Vaatamata tänapäevase arvutustehnika tohutule arvule uutele funktsioonidele ja võimalustele on Windowsi tuumi arhitektuur jäänud peaaegu muutumatuks.

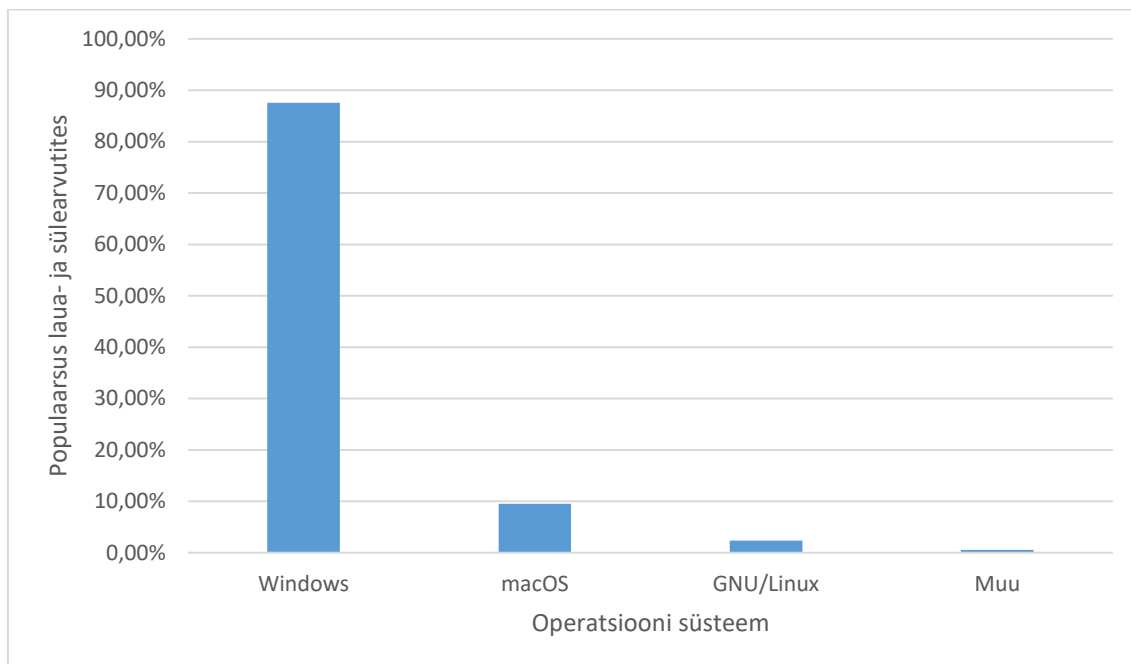
Macintoshi operatsioonisüsteem (lühend macOSst) on Apple'i väljatöötatud patenteeritud operatsioonisüsteem Macintoshi arvutites kasutamiseks. Vastavalt kasutajalepingule pole teiste tootjate seadmetel õigust seda süsteemi kasutada.

Linux on Unixi-laadsete operatsioonisüsteemide perekond, mis kasutab Linuxi tuuma, mille on arendanud Soome-Ameerika programmeerija Linus Torvalds. Süsteeme, mis kasutavad Linuxi tuumi, nimetatakse Linuxi distributsioonideks.

3.1.1 Turuosa

Windowsi nimetatakse tavaliselt algajate jaoks parimaks operatsioonisüsteemiks. Tänapäevasel statistika järgi umbes 85% koduarvutitest ja sülearvutitest kasutab seda operatsioonisüsteemi ning selle positsioon vastupidiselt mõnede ekspertide prognoosidele ainult tugevneb, samas kui macOS hõivab 9% turust ja Linux ainult 2%. Väike Linuxi osakaal on tingitud asjaolust, et enamiku tavakasutajate jaoks on Linuxiga töötamine palju keerulisem kui Windowsiga ja seetõttu on Linuxi kodutarbimise atraktiivsus väga piiratud. Linuxi põhisektor on serveritarkvara. See fakt tähendab ka

seada, et hoolimatute häkkerite sihtrühmaks on nende palju laiemat levitamist tõttu Windows või macOS.



Tabel 1. Operatsiooni süsteemide populaarsus *Netmarketshare* järgi

3.1.2 Tuum

Linuxis on kõik draiverid sisseehitatud tuumisse, aga enamik programme on kasutajaruumis, sealhulgas graafiline kest. Monoliitstruktuur annab suurema turvalisuse, sest kui keelata mooduli tugi tuumii loomise etapis, on koodi võimatu tuumi tasemel käivitada. See on võib-olla peamine erinevus Linuxi ja Windowsi vahel. Windowsil on täiesti erinev tuuma tüüp. Windows kasutab hübriidtuuma, mis koosneb paljudest väikestest osadest - *dll*-tekidest, millest igaüks vastutab rangelt oma funktsiooni eest.

MacOS kasutab ka hübriidset (XNU) tuuma, mis põhineb Mach'i mikrotoomal ja sisaldab Apple'i välja töötatud koodi.

3.1.3 Süsteeminõuded

Selles võrdluses võeti näiteks üsna populaarne Linux Mint Cinnamoni töölauakeskonnaga. Süsteemide miinimumnõuded võeti nende süsteemide avalehtedelt.

Võrdluseks näeme, et paljudes aspektides annab GNU / Linuxil põhinev süsteem parima tulemused. Korrektseks tööks vajaliku RAMi hulga osas tarbib GNU / Linux koos macOSga vaid 0,5 GB, mis on palju vähem kui Windows. Sama on ka pärast paigaldamist

hõivatud kettaruumiga. On näha, et isegi macOSga võrreldes võtab GNU / Linuxi süsteem peaaegu kaks korda vähem ruumi ja võrreldes Windowsiga on see neli korda vähem.

	MS Windows	macOS	GNU/Linux (Linux Mint)
Protsessor	1 GHz	867 MHz	x86 protsessor
Muutmälu	2 GB	512 MB	512 MB
Mälu	20 GB	9 GB	5 GB
Miinumum resolutsioon	800 x 600	-	800 x 600

Tabel 2. OSide miinumum süsteeminõuded

3.1.4 Esimene etappi kokkuvõtte

Lõpus saab ülaltoodud andmete põhjal koostada võrdleva tabeli. Selles tabelis lisan ka mõned aspektid, mis neid OSi eristavad.

	Windows	GNU/Linux	macOS
Turuosa	Kõige populaarsem operatsioonisüsteem. Liider töölaua segmendis. Saab kasutada palju erinevat tarkvara.	Väike turuosa, tulenevalt asjaolust, et GNU / Linux ei ole algajatele kasutajatele eriti sõbralik. Serverite segmendis väga populaarne.	Suhteliselt väike publik. Selle põhjuseks on asjaolu, et Apple ei luba OSi ametlikult paigaldada muudele toodetele kui Apple.
Tuum	Hübriid tuum	Monoliit tuum	Hübriid tuum
Failistruktuur	Windowsil on kataloogistruktuur, mis salvestab kasutaja erinevat tüüpi faile. On ka faile, mis võivad olla arvutustabel või rakendusprogramm. Sellel võib olla laiendeid <i>.txt</i> , <i>.jpg</i> jne.	Linux salvestab andmeid puu kujul. Seal on üks failipuu ja kõik teie kettad on paigaldatud selle puu kohale.	Failisüsteemil on puulaadne hierarhiline struktuur. Selle korraldamiseks kasutatakse katalooge - failisüsteemi objekte, mis sisaldavad faile ja muid katalooge.
Register	Windowsi register on peamine andmebaas, mida kasutatakse kõigi seadete salvestamiseks arvutisse. Ta vastutab kogu	macOS salvestab kõik rakenduse sätted <i>.plist</i> -failide seeriatesse. Need failid	Linuxil pole oma registrit. Kõik rakenduse seaded salvestatakse programmiliselt. Nende andmete salvestamiseks

	kasutajainfo salvestamise eest koos oma paroolide ja seadmeteabega.	sisaldavad kõiki atribuute teksti- või kahendvormingus.	puudub tsentraliseeritud andmebaas.
Süsteeminõuded	Suhteliselt kõrged süsteeminõuded, stabiilseks tööks nõuab palju RAMi ja võtab pärast paigaldamist päris palju ruumi.	Kulutab kõige vähem ressursse.	Suhteliselt madalad süsteeminõuded, kuid töötab kõige paremini Apple'i riistvaral.

Tabel 3. Süsteemide võrdlus

3.2 Teine etapp

Teine samm on nende operatsioonisüsteemide turvalisuse ja privaatsuse võrdlemine. Kahjuks pole praegu mõtet esitada mitmesugust statistikat nende operatsioonisüsteemide haavatavuste kohta, kuna enamikku sellist statistikat esitakse ebaõigesti ja ebaobjektiivselt. See küsimus nõuab eraldi kvalitatiivset uuringut.

3.2.1 Turvalisus

Suur põhjus, miks Windowsi peetakse vähem turvaliseks kui konkureerivaid OSi, ei tulene Microsofti turvastandardite ja uuenduste puudumisest, vaid selle suurest populaarsusest tõttu. Seda kasutavad nii koduarvutite tavakasutajad kui ka ettevõtete töötajad. Windowsi kasutavate inimeste arv on tohutu ja seetõttu on häkkerid kogu maailmas keskendunud sellele operatsioonisüsteemile rohkem kui teistele. Windowsis saavad pahavara ja viirused üsna hõlpsasti juurdepääsu süsteemifailidele ja võivad palju kahjustada. Lisaks luuakse Windowsi all maksimaalne viiruste arv. Märgin, et Linux ei ole kaitstud ka rünnakute vastu süsteemile, aga kui järgite lihtsamaid reegleid ja ei anna ülekasutajale õigusi kõigele, mida käitate, siis olete tõenäoliselt turvalisem kui Windows.

Samuti väärrib märkimist, et Microsoft vabastab oma Windowsi värskendusteenuse kaudu regulaarselt turvapaiku. Neid antakse välja umbes kord kuus, kuigi kriitilised värskendused on saadaval lühemate intervallidega.

System Integrity Protection (SIP) on Apple macOS-i operatsioonisüsteemi turvaelement, mis võeti kasutusele OS X El Capitanis 2015. aastal. See koosneb paljudest mehhanismidest, mida tuum tagab. See kaitseb muudatuste eest, mis toimuvad ilma konkreetse õigusetähta protsesside poolt, isegi kui need täidab juurkasutaja või *root*-

õigustega kasutaja. MacOSSis pööratakse palju tähelepanu Apple'i kaubamärgiga riistvarale. Apple T2 turvakiip, mis on varjatud paljude uuemate Mac-mudelitega, hoiab Mac OSi turvalisena. Apple T2 kiibi kaasprotsessor *Secure Enclave* on Touch ID, turvalise alglaadimise, *FileVault* ja krüpteeritud salvestusvõimaluste alus.

Kui arvestada Linuxiga, siis on isikuandmete asjakohase turvalisuse ja konfidentsiaalsuse taseme säilitamine selle operatsioonisüsteemi põhimõtte. Vaikimisi pole tavakasutajatel juurjuurdepääsu ega administraatoriõigusi. Ja kuna Linuxi tuum on avatud lähtekoodiga ja süsteemi ennast haldab kogukond ning seda jälgivad regulaarselt arendajad üle kogu maailma, saab kõik tekkinud probleemid mõne tunni jooksul lahendada, saades vajaliku paranduse parandusega. Seetõttu on Linux IT-spetsialistide seas nii populaarne.

Paljud inimesed arvavad, et oma arhitektuuri ja kasutajaõiguste käsitlemise tõttu on Linux turvalisem süsteem kui Windows ja macOS. Linux ei töötle käivitataavaid faile ilma selge loata.

	MS Windows	GNU/Linux	macOS
Root õigused	Administraatori õigused pole alati usaldusväärset kaitstud	Unix-like põhimõtted Kasutaja alati kontrollib kuhu ja mis protsessile ta annab admini õigused.	Unix-like põhimõtted
Protsesside isoleerimine	Windowsi konteinerite jaoks on kaks erinevat käituse isoleerimisrežiimi: protsesside eraldamine ja Hyper-V isoleerimine.	Võib paigaldada erinevaid isoleerimise ja virtualiseerimise keskkonnad (<i>chroot</i> , <i>cgroups</i> jne)	Kõik programmid on isoleeritud.
Arhitektuur	Tuum ja API töötavad tihedalt. Tuumis võivad tekkida probleemid kui tekib mingi tõrge API-s	Tuum ja API töötavad eraldi	Tuum ja API töötavad eraldi
Brandmauer/ Tulemüür	Microsofti Windowsi sisseehitatud tulemüür - Windowsi tulemüür on osa Windowsi turbekeskusest.	Integreeritud <i>iptables</i> <i>firewall</i>	Puuduvad integreeritud tulemüürid. Saab paigaldada.
Ressursside limiteerimine	-	Võib anda limiidi protsessi täitmisele.	-

Tabel 4. OSide erinevused turvalisuses

3.2.2 Privaatsus

Paljud inimesed ei saa tänapäeval aru turvalisuse ja konfidentsiaalsuse või privaatsuse [3] erinevusest. Nende jaoks privaatsus on turvalisuse tagajärg, see tähendab, et kui suhteliselt turvaline operatsioonisüsteem, nagu näiteks macOS, ei luba pahatahtlikel komponentidel varastada andmeid pahatahtlikel eesmärkidel või lihtsalt ilmuda, ei tähenda see, et nende andmed ei satu kolmandate isikute kätte. Järgmisena tahan anda teavet erinevatest juhtumitest avatud allikatest, mis on avalikkusele kättesaadav.

3.2.3 MS Windows

Windowsi operatsioonisüsteemi ja selle omaniku Microsoftiga on seotud palju erinevaid juhtumeid, kus nad tabati andmete kogumiselt enda ja teiste kasutajate kohta. Näiteks sunnib Microsoft ühes oma uuenduses Windowsi kasutajaid paigaldama uuendusi, mille ettevõtte kehtestab oma universaalsete lünkade kaudu. Need uuendused võivad kasutajatele mitmesugust kahju tekitada, näiteks piirata mõningaid arvutifunktsioone või sundida kaitsetuid kasutajaid tegema kõike, mida Microsoft ütleb [4]. Või Windowsi paigaldamisel luua Microsofti konto, kuhu peate sisestama konfidentsiaalsed kasutajaandmed. Microsoft ei paku selle sammu vältimiseks ühtegi võimalust. Muidugi saab seda vältida, kui keelate operatsioonisüsteemi paigaldamise ajal juurdepääsu Internetile, kuid see samm pole tõenäoline ja tavakasutaja loob pigem konto ning annab seeläbi kolmandatele isikutele juurdepääsu nende konfidentsiaalsele teabele [5].

Ülaltoodud näited on avaldatud ilma Microsofti teadmata. Kuid Microsoft ise ütleb otse, et kogub palju konfidentsiaalset teavet [6]. Näiteks öeldakse Microsofti privaatsusavalduses [7]: „Milliseid andmeid kogume, sõltub teie ja Microsofti vahelise suhtlemise kontekstist ja tehtavatest valikutest (sh privaatsussätetest) ning kasutatavatest toodetest ja funktsioonidest. Teiega seotud andmeid kogume ka kolmandatelt osapooltelt.“ Kahjuks on pärast rohkeid uurimisi sellel teemal leidnud kasutajad ja kvalifitseeritud teadlased, et isegi pärast pikka ja vaevarikast protsessi, mille käigus Microsoftile oli keelatud juurdepääs eraandmetele [8] [9], saadetakse endiselt palju tundmatut teavet nii Microsoftile kui ka kolmandatele osapooltele.

Microsofti privaatsusavaldusest on selge ka, et ka nemad ei kõhkle kolmandatelt isikutelt mitmesuguse teabe saamisel, millest võime teha väikese järelduse, et „infoturg“ püsib aktiivne ja isegi kasvab. Selles infokogus ei ole arvestatud Microsofti korporatsiooni

varalisi tooteid, mis omakorda koguvad aktiivselt teavet ka kasutajate kohta [10] [11] [12].

3.2.4 macOS

Ükskõik kui kõvasti üritab Apple meid veenda, et nad seavad meie privaatsuse ja privaatsuse üle kõige, et saame nende tooteid ohutult kasutada, on kahjuks nende toodetega seotud palju juhtumeid. Nende varalises operatsioonisüsteemis oli näiteks hiljuti juhtum [13], kui sai teatavaks, et macOSi saadab Apple'ile iga programmi käivitamisel *hash* (kordumatu identifikaatori). Paljud inimesed polnud sellest teadlikud, kuna *hash* edastatakse nähtamatult ja ainult interneti ühenduse olemasolul. Üllatav oli, et edastati need *hash* 'id kolmanda osapoole ettevõtte kaudu krüpteerimata.

3.3 Võrdluse kokkuvõte

Tahaksin öelda, et minu toodud näited avaldasid kasutajad ja teadlased, kes olid huvitatud privaatsuses ja turvalisuses. Kõige kurvem on see, et kui mitte nemad, siis poleks me teada saanud, mis nendes varalistes operatsioonisüsteemides meie andmetega toimub. Nende omanikud on väga huvitatud igasugusest meie kohta käivast teabest ega kõhkle seda isegi teistest allikatest. Loomulikult pidid ettevõtted pärast nende juhtumite avalikustamist need lüngad, vead või *backdoor*'id parandatud. Kuid nagu näeme, ilmuvad pärast seda teised, mida on veelgi raskem ära tunda. Ja see pole veel puudutanud nende samade ettevõtete toodetega kaasas oleva tarkvara teemat ning erinevate lepingute ja litsentsilepingute juriidilisi tingimusi, mille kasutaja allkirjastab nende varaliste operatsioonisüsteemide kasutamise hakkamisel. Eeltoodu põhjal näete, et varalised OSid pole minu töös head võimalused privaatses ja konfidentsiaalses keskkonnas ning seetõttu valin ühe minu vajadustele vastava GNU / Linux'i distributiiv.

4 Linuxi privaatsed distributiivid

Töö selles osas tuuakse näiteid turvalisusest ja privaatsusest, mis on erinevates distributsioonides ja mille funktsioone saab käesolevas töös kasutada.

Otsustati kasutada portaali *DistroWatch*. *DistroWatch* on teabe- ja uudiste veebileht erinevate Linuxi distributsioonide ning muude vaba ja avatud lähtekoodiga operatsioonisüsteemide, näiteks OpenSolaris või BSD kohta. Portaal jälgib distributsioonide kirjeldusega leheliikluse pingerida, mis on ligikaudne viis nende populaarsuse hindamiseks. Selle portaali distributsioonide otsingus kasutati filtrit, mis näitab suurenenud kaitse ja privaatsusega distributsioon. Nende hulgas võib märkida järgmisi distributsiooneid.

4.1 Tails

Minu arvates on see distributsioon turvalisuse ja privaatsuse / anonüümsuse mõttes üks paremaid. Tails on Debiani põhine Linuxi distributsioon, mis on loodud privaatsuse ja anonüümsuse huvides. Kõik väljuvad ühendused on pakitud Tor-võrku ja kõik mitteanonüümsed ühendused on blokeeritud. Süsteem on loodud käivitamiseks LiveCD / LiveUSBst ega ei jäta jälgi masinas, milles seda kasutati [14]. Tori projekt on Tailsi peamine sponsor. Operatsioonisüsteemi soovitas kasutada *Free Press Foundation* ja seda kasutas ka Edward Snowden [15]. Kogu süsteem töötab Live-režiimis ja laaditakse RAMi, Tailsi ei laadita HDDle, seda tehakse nii, et pärast seansi lõppu on võimatu kindlaks uurida, mida kasutaja arvutis tegi.

Seda operatsioonisüsteemi kategooriliselt ei arvestata kõvakettale paigaldamiseks kui püsivat operatsioonisüsteemi. Pärast süsteemi sulgemist või taaskäivitamist kõik allalaaditud failid, veebilehitseja ajalugu jne kustutatakse. Võite luua krüpteeritud partitsioon (*persistent*) ja sinna salvestada erinevat tüüpi paroole ja faile, kuid need failid ei pea olla suure konfidentsiaalsusega. Kuid sellel distributsioonil on oma puudused, mille tõttu pole mõtet seda oma töös kasutada. Esiteks ei ole selle kasutatav liides algajatele eriti hea. Teiseks, see ei sobi püsisüsteemina - on andmete kadumine võimalik

jne. See on lihtsalt kohandatud konkreetsete ülesannete jaoks, mis tavakasutajale ei ole vaja. Muidugi on see anonüümne ja hea turvaline süsteem, kuid on palju mugavamaid distributsiooni.

4.2 Linux Kodachi

Linux Kodachi on Debiani-põhine distro, mis pakub anti-kriminalistlik usaldusväärset anonüümset / turvalist operatsioonisüsteemi. Tema missiooniks on pakkuda võrgule kõige anonüümsemat ja turvalisemat juurdepääsu ning kaitsta süsteemi. Kodachis sunnitakse kogu liiklus läbi VPNi, seejärel läbi DNS-krüpteeritud Tor-võrgu.

Kodachit turustatakse kohtuekspertiisi vastase arendusena, mis raskendab draivide ja RAMde kohtuekspertiisi analüüsi. Kodachi on läbimõeldum kui Tails. Töölaua keskkonnaks valiti XFCE, süsteemi disain on väga sarnane macOSile.

Kodachile integreeritud protokoll ja haldusvahendi DNSCrypt, mis krüpteerib päringuid OpenDNSi serveritele elliptilise krüptograafia abil. See kõrvaldab mitmed levinud probleemid, nagu näiteks DNSi lekkimine ja võrguaktiivsuse jälgede jätmine Interneti-teenuse pakkuja serveritesse.

Kui peate P2P-võrkudes IP-aadressi peitma, võite kasutada PeerGuardian. Protsesside isoleerimine toimub kasutades sisseehitatud liivakasti Firejail.

Kodachil on palju eelpaigaldatud tarkvara mis tahes ülesannete lahendamiseks, näiteks teabe krüptimiseks (VeraCrypt), konfidentsiaalsete sõnumite edastamiseks (GnuPG, Enigmail, Seahorse, GNU Privacy Guard Assistant), jälgede varjamiseks (Nepomuk Cleaner , Nautilus-wipe, BleachBit)

Lisaks on Kodachil oma veebilehitseja, mis põhineb Tor veebilehitsejal, millesse on sisse ehitatud parimad, aga probleemimoodulid välja lõigatud. Kuid jällegi, nagu ka Tailsi puhul, pole selle distributsiooni projektis kasutada. Meie sihtrühma jaoks ei too nii suur funktsionaalsus kasutajatele palju kasu, kuid võib ka eemale peletada.

4.3 Septor

Septor Linux on disto, mis pakub kasutajatele head keskkonda anonüümseks internetis surfamiseks. Septor on stabiilne ja usaldusväärne levitamine, mis põhineb Debiani GNU/Linuxil koos kohandatavate KDE Plasma töölaua ja Tori tehnoloogiatega.

Varasematega võrreldes pole sellel erilist funktsionaalsust. Selles jaotuses on paigaldatud palju tarkvara üsna turvaliseks ja anonüümseks Interneti surfamiseks.

4.4 Eitic hack süsteemid

Samuti on palju erinevaid levitamisi, mis on suunatud nn eetilisele häkkimisele. Need jaotused on mõeldud erinevate süsteemide turvalisuse testimiseks. Meie töös on jällegi nendel jaotustel liiga palju funktsionaalsusi, mis jäävad lihtsalt üleliigseks.

Nendest süsteemidest on kõige populaarsemad näiteks Parrot Security, Kali Linux.

Kali Linux on eetilise häkkimise ja levitamise testimiseks kõige populaarsem operatsioonisüsteem. See distro põhjendatud Debiani põhjal. Esimene versioon ilmus 2006. aasta veebruaris BackTrack Linuxi perekonna asendamiseks.

Lisaks on Kalil üks suurimaid repositooriumid, kust leiate tööriistu mis tahes ülesande täitmiseks.

Parroti distro panustab turvakogukonda sama palju kui Kali Linux koos paljude häkkimistöööriistade ja suurepärase GUIga. Kali suurusega võrreldav repositoorium, mis sisaldab palju suurepäraseid häkkimistöööriistu algajatele ja ekspertidele. Esimene väljaandmine toimus 2013. aasta juunis. Nagu Kali, põhineb see Debianil ja kasutab graafilise keskkonnana MATE.

4.5 Kokkuvõtte

Vastavalt antud andmetele saab koostada privaatsuse ja turvalisuse tagamiseks loodud populaarseimate jaotuste võrdleva tabeli.

	Tails	Kodachi	Septor
Töölauakeskkond	GNOME	XFCE	KDE Plasma

Mis distro põhjendatud	Debiani põhjal	Xubuntu (Ubuntu) põhjal	Debiani põhjal
Vaikimisi paigaldatud veebilehitseja	Tor Browser	Sphere Tor Browser, Firefox	Tor Browser
Rakenduste isoleerimine	Sisse ehitatud "AppArmor"	Sisse ehitatud "FireJail"	Puudub, aga saab paigaldada
Mälu kustutamine sulgemisel	Mälu kustutamine sulgemisel ja hädaseiskamisel	Mälu kustutamine sulgemisel	-
Sisse ehitatud VPN	-	Tasuta VPN teenus	-
Sobivus kõvakettale paigaldamiseks	Võimalus on, aga ei ole soovitatav	Jah	Jah
Võimalus LiveCD luua	Jah, soovitatud kasutada ainult LiveCD kaudu	Jah	Jah
Muu	Kasutamine kõige mõistlikum mälupulga kaudu	Multi DNS, Süsteemi paraametreid ja turvaalisuse info töölaual	Suunatud veebisufmisele

Tabel 5. Distributiivide võrdlev tabel

Tehtud analüüsi põhjal võime järeldada, et turvalisuse ja privaatsuse suurendamisele suunatud distrod on projekti sihtgrupi jaoks liiga keerulised ja neil on liigne funktsionaalsus. Seetõttu peame kasutama lihtsamat distro, mis töötab hästi koos ID-kaardi tarkvaraga, mugava keskkonnaga ning hõlpsasti õpitav ja sihtrühmale arusaadav.

5 Nõuded privaatsusele ja turvalisusele

Esitatud teabe põhjal saab koostada loetelu olulisematest kriteeriumidest, mis mõjutavad turvalisusele ja privaatsusele.

5.1 Vabavaraligus

Esimene ja peamine kriteerium on vabavaraligus. Eeltoodud põhjustel võime järeldada, et ükski patenteeritud operatsioonisüsteem ja tarkvara ei taga piisaval tasemel konfidentsiaalsust, anonüümsust ja turvalisust isegi põhitasandil. Vastavalt *Free Software Foundation*'le [16] [17] andmetel on programm tasuta ja mitteomand, kui selle kasutajatel on neli põhivabadust:

- vabadus käitada programmi oma äranägemise järgi mis tahes eesmärgil.
- Vabadus teada, kuidas programm töötab, ja muuta programmi, et teha arvutusi nii, nagu soovite. See eeldab juurdepääsu lähtekoodile.
- Vabadus jagada koopiaid teiste abistamiseks.
- Vabadus oma muudetud versioonide koopiaid teistega jagada. Seda tehes saate kogu kogukonnale anda oma muudatustest kasu. See eeldab juurdepääsu lähtekoodile.

5.2 Kaitstud veebilehitsejad

Nagu eespool öeldud, ei tohiks tarkvara olla varaline. Sama lugu on veebilehitsejadega. Isegi pealtnäha populaarsel ja üsna usaldusväärsel Firefox'i veebilehitsejal on teatud kalduvus meie privaatsust rikkuda. Näiteks on isegi nende veebilehitseja privaatsuspoliitikas kirjas, et nad koguvad vaikimisi meie kohta palju teavet [18].

Kõige kuulsam ja populaarsem veebilehitseja millel on kaitstud maine on Tor. On ka teine konfidentsiaalne veebilehitseja - Brave. See on tasuta ja avatud lähtekoodiga veebilehitseja, mis põhineb Chromium'i veebilehitsejal. See hakkas toetama IPFS-tehnoloogiat [19]. Kuid meie töös on veebilehitseja valimisega seotud mitu piirangut. Esimene on võimalus kasutada ID-kaarti igapäevatoos. Aga see ei tööta Toriga

korralikult. Teine piirang on meie sihtrühma kasutajate mugavus, kuid kahjuks on Tor suunatud pigem edasijõudnutele. Selle põhjal võime järeldada, et töös saab kasutada veebilehitsejat Brave, kuna see vastab kõigile meie sihtrühma kriteeriumidele - piisav turvalisus, anonüümsus, vabavaraline ja toetab ID-kaardi.

5.3 Incognito režiim

Vaikimisi kasutavad paljud veebilehitsejad tavalist kasutusrežiimi, mis salvestab meie kohta palju teavet, näiteks erinevaid logisid, sirvimisajalugu ja kui kasutaja lubab, siis paroole ja sisselogimisi. See režiim pole absoluutselt konfidentsiaalne ega ei vasta töö nõuetele. Selle põhjal on vaja määrata vaikimisi inkognito režiimi, millel on eraldi isoleeritud veebi surfamise ajalugu - sealhulgas küpsised, automaatsed vormid. Kettavahemälu kasutatakse minimaalselt ja see kustutatakse väljumisel.

5.4 Privaatne otsingumootor

Populaarsed otsingumootorid nagu Google, Yahoo, Yandex jt jälgivad, ekstrakteerivad ja profiilivad teie otsinguid, et reklaamijad saaks teile pakkuda mingi kaup miljonite veebilehitsejate sisse ehitatud tohutute reklaamivõrgustike kaudu [20]. Vähemalt see asi kinnitab, et populaarsed otsingumootorid on enamikus mittekonfidentsiaalsed. Hetkel kõige privaatsust teadlikum ja kasutajasõbralikum on *DuckDuckGo.com*. See on ennast tõestanud otsingumootorina, mis ei kogu kasutajate kohta mingit teavet. Töös peaks see otsingumootor olema paigaldatud veebilehitsejasse vaikimisi.

5.5 Lõikepuhvri kustutamine

Viimasel ajal on tekkinud palju rakendusi, mis kasutavad lõikepuhvrit. Konfidentsiaalse teabe ründajatele edastamise riski vähendamiseks on vaja luua automaatse lõikepuhvri iga minutine kustutamine.

5.6 Tehtavad tegevused ei salvestu

Kuna süsteem peaks olema võimalikult konfidentsiaalne, tähendab see, et pärast arvuti väljalülitamist või mälu pulga eemaldamist ei tohiks arvutisse jääda mingeid andmeid. Tuleb luua viimase seansi ajal tehtud muudatused automaatne kustutamine.

6 Linux Mint

Analüüsi käigus saadud andmete, populaarsete jaotuste võrdlemise ja tehtud järelduse põhjal võime öelda, et privaatsuse ja konfidentsiaalsuse tagamise eesmärgil loodud jaotused ei vasta töö nõuetele. Otsustas valida ühe vähem spetsialiseerunud jaotuse hulgast. Distrowatchi järgi on hetkel kõige populaarsemad Ubuntu ja Linux Mint. Mõlemat süsteemi on lihtne paigaldada ja nende seadistamiseks pole vaja eriteadmisi. Seetõttu on algajatele kasutajatele sageli soovitatav just neid OSi, et alternatiividele üleminek oli üsna lihtsaks. Linux Minti distributsioon on ümber töötatud Ubuntu. Selle sisemine struktuur on sarnane, kuid graafilises liideses, põhiprogrammide komplektis ja kasutajaga suhtlemise viisides on erinevusi.

Ubuntul võib olla mitmesuguseid töölauakeskkondi, millest kõige populaarsemad on GNOME ja UNITY. Need keskkonnad pole eriti kasutajasõbralikud, kuid on üsna ilusad ja kaasaegsed.

Samuti Linux Mint tehakse Ubuntu LTSi põhjal. LTS on rohkem testitud ja seetõttu ka töökindlam.

Linux Mint pakub mitmesuguseid Linuxi töölaua keskkondi, kuid vaikimisi on Cinnamon. See keskkond sarnaneb pigem Windowsi liidesega, mida enamik personaalarvutikasutajaid kasutavad. Samuti see keskkond produktiivsem kui need, mis pakub Ubuntu. Ametlikul Linux Minti veebisaidil on ka võimalus alla laadida MATE ja XFCE keskkondadega versioonid, mida saab kasutada projekti edasiarendamisel.

Privaatsuse osas mõlemal OSil on erinevusi. Kuna Ubuntut arendab äriettevõtte Canonical, Ltd., oli selles varem reklaame. Nüüd pole reklaame enam, kuid pole teada, mida tulevik toob. Linux Mint ei kannata neid puudusi, süsteem on erinevatest reklaamimoodulitest täiesti puhas. Lisaks Ubuntu kasutajalepingus, on pealkirjad et osa isikuandmetest edastatakse Canonicalile. Muidugi saab selle seadetes keelata, kuid ka Linux Mintil pole siin probleeme.

Eeltoodu põhjal otsustati töös valida Linux Mint.

7 Tingimused

Vastavalt ülikooli nõuetele, mugavusele ja ohutusele on vaja luua ISO-fail järgmiste kriteeriumidega.

ISO-fail peab olema:

- Luuakse USB-pulgale paigaldatav alglaaditav ISO-fail
- ISO-fail töötab nii BIOS kui UEFI režiimis
- Luuakse SHA256 kontrollsumma

Operatsioonisüsteem peab olema:

- Vabavaraline
- Kõrgendatud turvalisuse ja privaatsusega
- Võimalus see valitud OS paigaldada püsivalt arvutisse koos täiendavate turva- ja privaatsuse sätetega
- Võtaks võimalikult vähe riistvararessurssi

Samuti oli määratud erinevad kriteeriumid tarkvarale, kujundusele ja funktsionaalsusele, mis peavad olema selles OSis:

- Veebilehitsejale on lisatud ülikooliga seotud lingid
- Saadaval on ka veebilehitseja *tor*-režiim
- Ülikoolile sobiv taustapilt lisatud
- Toimib eesti ID-kaarditarkvara

Kõrgendatud turvalisuse ja privaatsuse aspektid:

- Veebilehitseja käivitub vaikimisi privaatses režiimis
- Vaikimisi on veebilehitsejas privaatne otsingumootor

- Tehtavad tegevused ei salvestu (kustuvad OSi sulgemisel)
- Käsurea ajalugu on vaikumisi keelatud
- Lõikepuhvri sisu kustub määratud aja (nt 1 min) jooksul

8 Tulemused

8.1 Koodi jagamine

Edasiseks arendamiseks ja ka skriptile juurdepääsuks peaks kõigile olema määratud veebiteenus projekti majutamiseks. Teenus peaks olema tasuta, populaarne ja mugav. Ideaalne kõikide parameetrite jaoks on GitLab. See on vabavaraline veebiteenus avaliku lähtekoodiga. Link GitLabile on allikates [21]. See veebiteenus annab järgmised võimalused:

- Saab luua erahoidlaid, mis on nähtavad ainult omanikule või valitud inimestele
- Hoidlatega on võimalik töötada teenuse veebiliidese kaudu
- Lisaks koodi postitamisele saavad osalejad suhelda ja kommenteerida üksteise muudatusi

Sinna lisati nii skript ise kui ka lisamaterjalid mälu pulga loomiseks.

8.2 Skripti kirjeldus

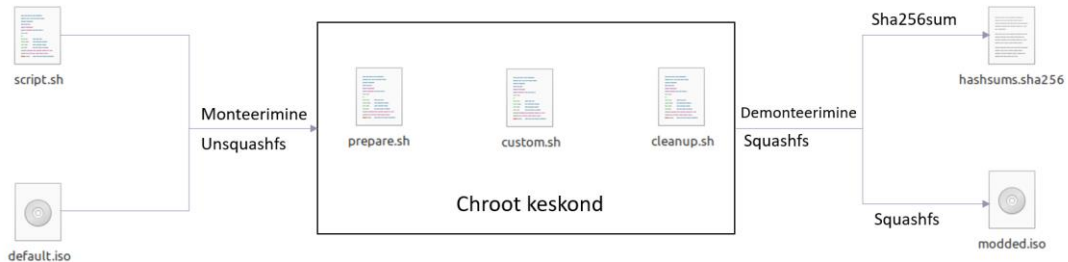
ISO-faili loomiseks on vajalik, et koos kaustas oleva skriptiga oleks vaikimisi Linux Minti ISO-fail Cinnamoni töölaua keskkonnaga, mille saab alla laadida distro ametlikult veebilehelt.

ISO-faili loomiseks otsustati kasutada järgmistest sammudest koosnevat meetodit:

- ISO-faili ühendamine (*mount*) ja lahti pakkimise protsess
- Vajalike moodulite paigaldamine
- Kohandamine ja muutmine
- Ühendamine ja puhastamine
- Uue ISO-faili loomine
- Kontrollsumma loomine

- Üldine puhastamine

Neid etappe saab paigutada skeemina.



Joonis 1 Skripti visuaalne vaade

Tulenevalt asjaolust, et see ISO-faili genereerimise skript käivitatakse Linuxis, otsustatud kasutada Bashi käsukeelt. See on keel, mis vaikimisi kasutatakse paljudes UNIXi-tüüpi süsteemides. Seetõttu skripti interpretaator `!/bin/bash`.

8.2.1 ISO ühendamine ja lahti pakkimine

Enne ISO-faili loomise protsessi peaks paigaldama süsteemivärskendused ja mõned paketid, mida skriptis kasutakse.

Kõigepealt tuleks igaks juhuks kustutada kõik kaustad ja kataloogid, millel on nimed *edit*, *extract-cd*, *mnt*, *squashfs* ja *squashfs-root*. Ennem kustutamist on parem veenduda, et neis pole midagi olulist. Siiski on parem luua eraldi kaust, kus kõik toimingud tehakse.

Pärast ettevalmistustööde lõppu Linux Minti *default image* mis laaditakse alla ja asub skriptiga samas kaustas paigaldatakse loodud kaustasse *mnt /*.

Nüüd peaks looma kausta *extract-cd* ja kopeerima sinna kausta *mnt /* sisu, välja arvatud pakitud failisüsteemiga fail *filesystem.squashfs*. Failisüsteemi lahtipakkimine toimub haldusvahendi *squashfs-tools* abil. Saadud andmed kantakse kausta *edit*, kus toimuvad ISO-faili peamised muudatused. Viimasena toimub *chroot*-keskkonna jaoks seadmete ühendamine.

See lõpetab ISO-faili sisuga töötamise ettevalmistamise etapi. Edasi tuleb töö ajutiste skriptifailide loomiseks mis hakkavad *chroot* keskkonnas käivitatakse.

8.2.2 Skript moodulite ja DNS-serveri ühendamiseks

Esimene fail *prepare.sh* ühendab hostisüsteemi olulised kataloogid *proc*, *sysfs* ja *devpts* redigeerimise kataloogisse (*edit*). Samuti luuakse muutujad *HOME* ja *LC_ALL* eesmärgiga vältida probleeme *locale*'ga ja GPG võtmete importeerimisel. Interneti-ühenduse säilitamiseks *chroot*-keskkonnas peaks lisama DNS-serveri IP. Meil see on 8.8.8.8.

8.2.3 Skript süsteemi konfigureerimiseks ja muutmiseks

See skript on konfigureerimiseks. Sellega tehakse läbi *chroot*-keskkonna ISO-faili põhilised muudatused. Näiteks tarkvara värskendamine, vajalike programmide paigaldamine, konfiguratsioonide muutmine, välimuse muutmine ning tarbetute komponentide ja programmide eemaldamine. Samuti on vaja rakenduse konfiguratsioonide jaoks looma *.locale-s* uue kataloogi, kuhu paigutatakse kõik muudetud või kohandatud konfiguratsioonifailid.

8.2.4 ID-kaardi tarkvara paigaldamine

Pärast süsteemi komponentide värskendamist võib alustada vajalike programmide paigaldamisega. Esimene neist on ID-kaardi tarkvara. Selle paigaldamiseks peate tegema mitu toimingut.

- Paigaldusfaili allalaadimine
- Paigaldusfaili muutmine
- Paigaldusfaili käivitamine
- Puhastamine

Esimene on alla laadida paigaldusfaili uusim versioon ametlikult veebilehelt id.ee. Kui see on tehtud, on vaja kustutada rida, mis initsialiseerib testi *root*'i kontrollimiseks. Meie puhul pole seda testi vaja läbida, seetõttu kustutame mittevajalikud ridad *sed* abil ja kirjutame uude faili.

Nüüd saab käivitada uue faili ja pärast paigaldamist eemaldada kohe kõik mittevajalikud failid.

8.2.5 Veebilehitseja Brave

Veebilehitseja paigaldusprotsessis pole praegu midagi keerulist. Esimene samm, nagu arendaja soovib, on *curl* paketi paigaldamine, kui see pole veel paigaldatud. Seejärel laaditakse alla vajalikud GPG-võtmed. Viimane on konfiguratsioonide värskendamine ja veebilehitseja paigaldamine.

8.2.6 Incognito mode vaikimisi

Nagu tingimustes kirjutati, on üks olulisi meetodeid kasutajate andmete privaatsuse ja turvalisuse tagamiseks on inkognito režiimi kasutamine. Peame selle vaikimisi määrama veebilehitsejatele, mis on meie süsteemi ISO-failis. Selleks muudetakse nende veebilehitsejate konfiguratsioonifaile. Neid ridu, mis algab *Exec'ga* failides *firefox.desktop* ja *brave-stable.desktop*. Samuti oleks tore lisada lisaks inkognito režiimile veel üks võimalus. Selleks, et paroolihaldur tulevikus ei häiri meid kogu aeg, võib selle keelama, lisades lõppu *--password-store = basic*.

8.2.7 Lõikepuhvri kustutamine

Vastavalt töötingimustele on vaja lõikepuhvri teatud ajavahemiku järel automaatselt puhastada. Selleks otsustati kasutada CRON-haldusvahendi. Selleks luuakse fail *clipboard.sh*, mis kustutab lõikepuhvri. Samuti antakse talle lubamine käivitamiseks. Pärast seda lisatakse see haldusvahendi konfiguratsioonifaili kirjele.

8.2.8 Teised asjad

Lõpus saaks lisada mitmesuguseid graafilisi funktsioone, muuta taustapilti, ja palju muud. Samuti keelatud vaikimise terminali ajalugu vaatamine. Muudetud töölaua taustapilti. Selleks laaditakse alla ülikooli kavandatud taustapilt TalTechi veebilehelt. Peaks laadi alla kausta */usr/share/backgrounds/linuxmint/*.

8.2.9 Puhastamine

Kui kõik ISO-faili muutmise tööd on lõpetatud, saab eemaldada programmid, mis ei huvita sihtrühmale, samuti tarbetud failid, mis võivad jääda.

8.2.10 Skript *chroot*'ist väljumiseks

Et tulevikus DNS-serveriga ühenduse loomisel probleeme ei tekiks, peab kustutama faili *resolv.conf* sisu. Samuti peate tühjendama kõik ajutised failid ja ka alla laaditud pakertifailid. Tuleb kasutada *apt purge*, et eemaldada paketid, mis laaditi teiste pakettide vajaduste rahuldamiseks automaatselt alla ja nüüd pole enam vajalikud.

8.2.11 *Chroot*'i käivitamine

Kui ettevalmistus-, seadistus- ja puhastus skriptid on edukalt loodud, saab neid järjest käivitada läbi *chroot*-keskkonna. Esimene peaks olema ettevalmistav fail, mis valmistab keskkonda seadistamiseks ette. Seejärel tuleb konfiguratsioonifail, tänu millele toimuvad keskkonnas muudatused. Ja viimane on puhastus skript, mis eemaldab kõik ebavajalikud kataloogidest, kuna ruumi on üsna vähe. Kui puhastustoimingu ajal ei olnud jaotist *edit / dev* lahti ühendatud, siis saab seda teha nüüd, mida teeb käsk *umount edit / dev*.

8.2.12 ISO loomine

Enne ISO-faili genereerimist tuleb teha veel paar asja. Failisüsteemi manifest tuleb ümber kirjutada. Selleks anname võimaluse teha faili *filesystem.manifest* kaudu kirjed *chmod + w* ja pärast selle ümberkirjutamist tagastame vanad õigused *-w*.

Kirjed sisaldavad andmeid, mis oli saadud *dpkg* andmebaasides loetletud pakettide kohta teabe lugemisel ja koosnevad kahest reast reast:

- Paketi nimi
- Paketi versioon

Samuti peab eemaldama vana tihendatud failisüsteemi. Pärast seda tihendame uus modifitseeritud versioon haldusvahendi *Squashfs-tool* kaudu, mida kasutasime lahtipakkimisel ja mille paigaldasime skripti alguses. Seda saab teha käsuga *mksquashfs*. Pärast seda peate veidi ootama, kuna see protsess ei ole väga kiire. Ja viimane - kokkupõrgete leidmise lihtsuse tõttu kustutame MD5 algoritmi järgi loodud kontrollsummad ja genereerime uued algoritmi SHA256 abil.

Kõik on nüüd valmis ISO-faili genereerimiseks [22]. Kasutati haldusvahendit *mkisofs*. Selle käsu käivitamisel lisati järgmised valikud:

- **-D** - See määrab, et mitte kasutada kataloogide sügavat ümberjaotamist, vaid pakkida need lihtsalt selliseks, nagu nad on.
- **-r** -Loob *Rock Ridge*'i protokollil kasutamisel SUSP- ja RR-kirjed, et kirjeldada faile ISO9660-failisüsteemi peal.
- **-V** - Määrab peaplokki kirjutatava köite ID. Meil nimi määratletud muutuja *\$NEW_NAME* väärtusega
- **-cache-inodes** – See valik on vaikimisi aktiivne kõigis *UNIX-like* operatsioonisüsteemides.
- **-J** - Loob Joliet kataloogikirjed lisaks tavalistele ISO9660 failinimedele. Vajalik Windows-NT või Windows-95 masinates.
- **-l** - Lubab täielikult failinimesid kuni 31 tähemärki
- **-c** - Määrab alglaadimiskataloogi tee ja failinime, mida alglaadimisketta loomisel kasutada. See valik on vajalik määrata ketta loomiseks. Meil määratakse *isolinux/boot.cat*
- **-no-emul-boot** - See parameeter määrab, et kasutatav *image* on mitteemuleeriv. Süsteem laadib ja täidab selle faili ilma kettale emuleerimise toiminguteta.
- **-boot-load-size** - Määrab "virtuaalsete" (512 baiti) sektorite arvu laadimiseks mittemuleerimisrežiimis. Vaikimisi laaditakse alla kogu alla laaditav fail. Mõni BIOS-id võib neid valesti interpreteerida, kui nende arv ei ole 4 ja selle pärast me määrame sinna arv 4. See annab võimalus korralikult töötada nii UEFI, kui BIOSga.
- **-o** - Faili nimi, kuhu ISO failisüsteemi *image* kirjutatakse. Meil määratakse *./\$NEW_NAME.iso* väärtus. './.' on pantud, sest et *mkisofs* käivitakse *extract-cd* kaustast.

Viimane asi, mida teha, on selle toiminguga käigus kasutatud moodulid lahti ühendada ja need eemaldada.

8.3 Mälupulga valmistamise meetod

Paljust käivitavate USB-draivide loomiseks mõeldud programmidest sobib hetkel programm Ventoy. See programm võimaldab teil hõlpsasti luua mitme käivitusega väikmäluseadme või välise USB-draivi. Pärast USB-draivi spetsiaalset ettevalmistamist peate lihtsalt vajalikud failid kopeerima. Järgmisena räägin teile üksikasjalikult haldusvahendi kasutamisest ja selle võimalustest. Just tema valiti mitmel põhjusel:

- Lihtne kasutada. Selle programmi paigaldamiseks ja käivitava USB-mälupulga loomiseks pole vaja erilisi teadmisi.
- Võimalus valida mitme ISO-faili vahel, mis on projekti edasisel arendamisel väga kasulik.

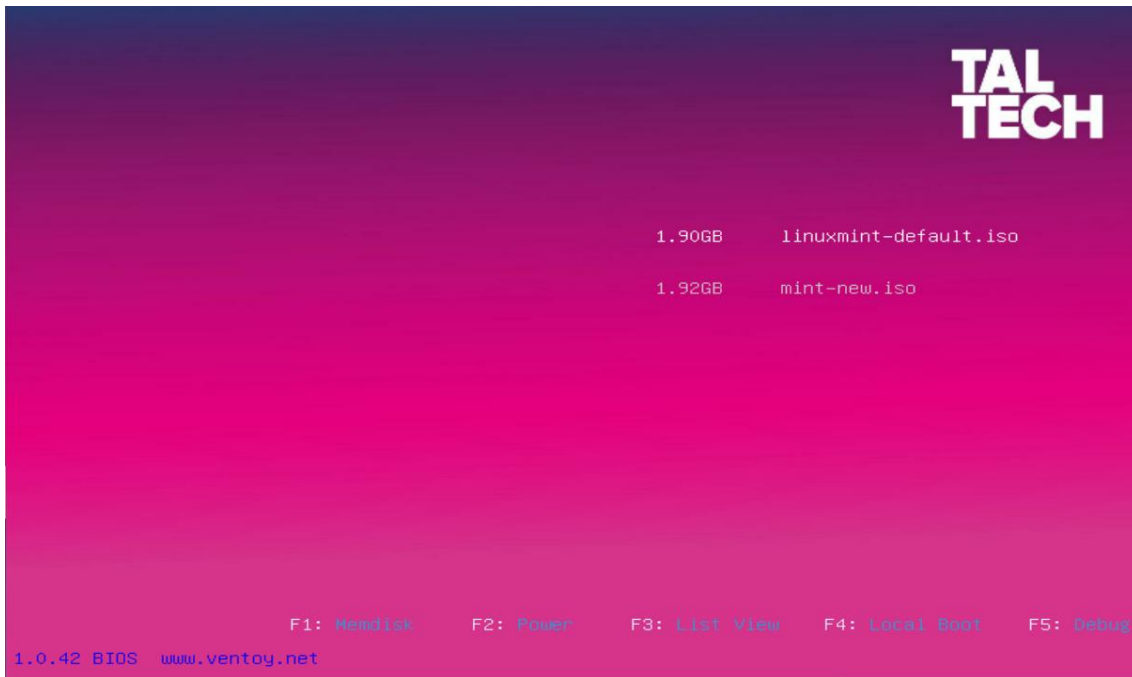
Niisiis, käivitava USB-draivi loomise protsess näeb välja niimoodi:

- Laadida Ventoy arhiiv alla programmi ametlikult veebilehelt [23] ja pakkige lahti see mugavale kohale
- Käivitage kaustast fail *Ventoy2Disk.exe*
- Valida *Options* aknas *Partition style* valik *MBR*.
- Valida programmi aknas soovitud mälupulk (kõik selle andmed kustutatakse).
- klõpsake nuppu *Install*
- Selle tulemusel jagatakse USB kaheks sektsiooniks
- Kopeerida vajalikud alglaaditavad ISO-failid.

Mälupulk on nüüd valmis. Saate muuta selle akna välimust, kus toimub valik ISO-failide vahel.

8.3.1 Ventoy välimuse muutmine

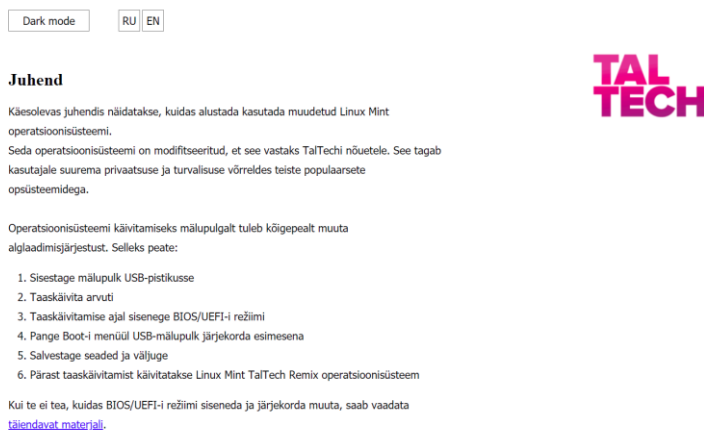
Vaikimisi kasutab Ventoy oma disaini, mis väliselt ei sobi projektile. Vaadet saab muuta - Ventoy annab selle võimaluse. Selleks on esimene samm alla laadida haldusvahend *MobaLiveCD*. Seal saab emulaatori abil testida käivitavat USB-mälupulka. Seda ei pea paigaldama. Peab lihtsalt käivitama faili *.exe* administraatori õigustega. Järgmisena tuleks luua vastavalt Ventoy juhistele oma välimusemuudatuste pakett. TalTechi logo taustapildid on lisatud ja saadaolevate ISO-failide loend on esteetilisema ilme saamiseks paremale viidud.



Joonis 2. Ventoy välimus

8.4 Juhendi loomine

Loodi juhend mälukaardi Ventoy'ga ja alla laaditud ISO-failiga kasutamiseks. Selleks kirjutati mitu faili *html*-formaadis. Kasutusjuhend on tõlgitud mitmesse keelde - vene ja inglise keelde. Lisatud on ka võime kasutada "tumedat režiimi". Selle juhendiga failid asuvad mälufulgal kaustas *Guide* ja neile viib seadme juure loodud otsetee.



Joonis 3. Juhend eesti keeles

9 Analüüs

9.1 Tulemuste analüüs

Töö käigus oli esitatud mõned põhjalikumad analüüsi nõudvad lahendused.

Nii näiteks skripti alguses on soovitatav, et ISO-fail oleks skriptiga samas kaustas. Tegelikult pole see vajalik, kuna saate skriptis määrata ka faili tee.

Tulevikus, kui ilmuvad uued Linux Mint versioonid või kui kasutaja otsustab mõne eelmise versiooni põhjal modifikatsiooni luua, peab ta skripti alguses muutma ka ISO-faili nime. Muidugi võiks luua faili otsing laiendiga *.iso*, kuid kui kaustas on rohkem kui üks ISO-fail, ei toimi automaatne failiotsing õigesti. Selleks saaks teha spetsiaalse skripti, mis kontrollib kõiki kaustas olevaid ISO-faile ja annab valiku, kuid siis läheb automaatika kaduma. Üldiselt on otsustatud jätta see element edasiarenduks.

Mõni sõna töölaua keskkonna versiooni kohta. Tulenevalt asjaolust, et selle projekti sihtrühmaks on enamasti Windows OSi kasutajad, tuleks neile pakkuda kõige tuttavam keskkond, milleks on Cinnamon. Sellest töölaua keskkonnas võivad kasutajad minna juba keerulisemale. Samuti pakub Linux Mint alla laadida veel kaks keskkonda - MATE ja XFCE. Need võivad tunduda Ubuntu kasutajatele tuttavad klassikalise GNOME'i keskkonna või macOS'i kasutajatega ning seetõttu saab neid kasutada edasiarenduses.

Edasi töö käigus otsustati jagada *chroot*-keskkonnas olevad käsklused mitmeks komponendiks - ettevalmistamine, kohandamine ja puhastamine. Seda tehti mitmel põhjusel. Esiteks on see veidi mugavam nii koodi lugemisel kui ka mis tahes komponentide muutmisel. Teiseks skripti muutmise ajal võib-olla tekib soov testida üksikuid komponente, mida saab faili lisada samamoodi või keelata ühte rida kommenteerides. Samuti on edasiarenduses võimalik, et skript muutub üsna suureks ja tuleb see jagada eraldi komponentideks, millest mõned on juba eraldatud, kuid on hetkel ühes failis.

Muudatuste skripti loomise alguses peaksite konfiguratsiooni failide salvestamiseks looma kaustas *.locale* koha. Seda tehakse seetõttu, et pärast rakenduste muutmist ei pruugi konfiguratsioone salvestada. Seetõttu kopeerime muudetud konfiguratsioonifailid kausta *.locale* või õigemini selle sees loodud *applications* kausta.

Kuna ID-kaardi tarkvara alla laaditud paigaldus fail sisaldab sisseehitatud testi, kas faili käivitatakse *root*'is või mitte, peame selle testi välja lülitada. Tulenevalt asjaolust, et kõik toimingud viiakse läbi *root*'na, ei võimalda see test meil tarkvara paigaldada.

Brave veebilehitseja paigaldamisprotsess oli selle arendaja soovitatud meetod. Selles protsessis laaditakse alla GPG-võtmed ja paigaldatakse rakendus.

Kõigi konfiguratsioonide lõpus kasutati *apt purge* haldusvahendi. Kuna ISO-faili ruum on piiratud, ei tohiks seal midagi täiendavat olla. Selle haldusvahendi abil eemaldame mitte ainult programmid ja nende konfiguratsioonifailid, vaid ka puhastame koht.

Pärast muudatuste tegemist oli vaja modifitseeritud süsteemi manifestifail ümber kirjutada. See on dokument, mis kirjeldab tarkvarapaketi manifesti või tarkvarade kogum. Seda kasutatakse mitmesuguse tarkvara lahti pakkimiseks ja konfigureerimiseks. Ja kuna meil oli uus tarkvara, oli vaja ka manifest ümber kirjutada.

ISO-faili loomisel kasutati haldusvahend *mkisofs*. On veel üks haldusvahend nimega *genisoimage*. Praegu on nad täiesti identsed. Ainukene asi, mis neid eristab, on see, et *mkisofs* on Linux Mintis vaikimisi paigaldatud ja seetõttu kasutasin seda, sest kogu protsess toimus selles OSis.

Mälupulgasse ISO-faili panemiseks valiti Ventoy. See tarkvara võimaldab teil USB-mälupulgale alla laadida mitu ISO-faili ja enne süsteemi käivitamist on võimalus valida, millist faili me käivitame. Samuti on suurepärase võimalus valikuekraani välimust kohandada. Ventoy on suurepäraselt sobib edasiseks arenguks.

9.2 Lähtetingimuste analüüs

Kolme põhiprobleemi lahendamiseks autori poolt määratud tingimused olid täidetud osalises või täielikus määras.

Käesoleva töö käigus loodi:

- ISO-fail, mida võimalik kasutada nii BIOSi kui UEFI režiimis
- Loodi automaatne skript koostab täiendatud ISO-faili
- Kasutatud operatsioonisüsteem ISO-failis on kõrgendatud turvalisuse- ja privaatsusega
- Kasutatud operatsioonisüsteem ISO-failis võtab suhteliselt vähe riistvararessursi
- Lisati kõrgendatud privaatsusega veebilehitseja
- Vaikimisi veebilehitseja käivitatakse tundmatu (incognito) režiimiga
- Veebilehitsejal lisatud lingid TalTechi ja IT kolledži veebilehtedele
- Lisati ülikooli taustapilt
- Lõikepuhvri sisu kustutakse ajastatud toiminguga (CRON) abil iga 1 minuti järel
- Muudeti Ventoy välimus
- Loodi manuaal

10 Tulevikuarendused

Töö käigus oli loodud prototüüp, mida saab edasiarendamisel täiendada ja muuta. Nii et näiteks veelgi täieliku turvalisuse ja privaatsuse tagamiseks võib ISO-faili konfiguratsioonis lisada komponente nagu RAMi automaatne puhastamine enne väljalülitamist või plaanimatu sulgemist. Ka tulevikus on võimalik luua veel mitu erineva töölaua keskkonnaga versiooni. Nii saaks näiteks luua XFCE keskkonnaga versiooni, mis on macOSi kasutajatele tuttavam. Seetõttu oli valiti Ventoy USB-mälupulka loomiseks.

Ka töö käigus selgus, et võrgus puuduvad kvalitatiivsed võrdlusuuringud erinevate OSide haavatavuse kohta. Asi on selles, et autori leitud uuringud pole objektiivsed ega kvaliteetsed. Seda saab kasutada lõputöö teemaks.

Tulevikus samuti saab skripti macOSi operatsiooni süsteemis – kas käivitakse õigesti ja kui seal mingi viga tekib siis parandada.

Samuti tulevikus on hea luua skripti automaattestimine.

Võiks ka muuta *Start* nupp alumise menüü ribal TalTechi disainiga nupule.

Selles projektis kirjutatud skript automatiseerib ainult muudetud operatsioonisüsteemi ISO-faili loomise. Praegu täieõigusliku käivitatava mälupulga loomiseks peab paigaldama Ventoy "käsitsi" ja kopeerima sinna kõik vajalikud failid ja kaustad, mis asuvad Gitlabis. Tulevikus saab lisada skripti, mis selle protsessi täielikult automatiseerib.

Kui projekt on lõpule jõudmas, tasub läbi viia ka uuring või küsimustik. On hea teada saada ülikooli PR-osakonna, sihtrühma arvamusi, nende arvamust tehtud töö kohta, rahulolematust, arvustusi mugavuse kohta jne.

12 Kokkuvõte

Bakalaureuse töö eesmärgiks oli skripti prototüüpi loomine. Diplomitöö tulemuseks oli ülikooli jaoks digitaalse võtme loomise kontseptsioon, mis sisaldab skripti ISO-faili loomiseks operatsioonisüsteemiga, millel on kõrgem turvalisuse ja privaatsuse tase. Samuti tehti valik mälu pulga valmistamiseks tarkvara.

Töö eesmärgi saavutamiseks oli korraldatud nii praktiline kui teoreetiline osad. Esiteks oli tehtud uuringulist osa, kus tõestati lõputöö probleemi aktuaalsuse olemasolu ja võrreldud populaarsemad operatsioonisüsteemid.

Töö teoreetilises osas tehti võrdlus, tänu millele leiti, et populaarsed operatsioonisüsteemid, nagu Windows ja macOS, on õigel kasutamisel küll suhteliselt ohutud, kuid privaatsusega on suuri probleeme. Peamine põhjus on see, et tegemist on varalise tarkvaraga. Seetõttu valiti tööks üks GNU / Linuxi distributsioonidest - eriti töötingimustele sobiv Linux Mint.

Töö praktilises osas loodi ISO-faili genereerimiseks vastavalt määratud parameetritele skripti prototüüp. Tulevikus saab seda skripti täiendada erinevate komponentidega ja käivitada täielikult automaatselt. Selle toimimiseks on vajalik, et skriptiga kaustas oleks originaalne ISO-fail, mille skript pakib lahti, muudab ja pakkib tagasi. Lõpus luuakse ISO-faili kontrollsumma.

Kirjeldati ka ülikooli "digitaalse võtme" osaks oleva USB-mälu pulga loomise meetodit. Selleks oli valiti Ventoy tarkvara.

Selle tulemusena võib öelda, et töö eesmärk on saavutatud, kontseptsioonil on õigus eksisteerida ja loodud projekti eeldused edasiarendamiseks.

Kasutatud kirjandus

- [1] U.S. Government Publishing Office, „Congressional Bills 112th Congress,“ 14 10 2011. [Võrgumaterjal]. Available: <https://www.govinfo.gov/content/pkg/BILLS112hres438ih/html/BILLS-112hres438ih.htm>. [Kasutatud 2021 04 01].
- [2] Netmarketshare, „Operating System Market Share,“ 17 04 2021. [Võrgumaterjal]. Available: <https://www.netmarketshare.com/>. [Kasutatud 16 04 2021].
- [3] FindLaw's team, „Is there a Difference Between Confidentiality and Privacy?,“ 18 03 2020. [Võrgumaterjal]. Available: <https://www.findlaw.com/criminal/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html>. [Kasutatud 02 04 2021].
- [4] B. A. Roston, „SlashGear,“ 18 10 2020. [Võrgumaterjal]. Available: <https://www.slashgear.com/windows-10-users-are-grumpy-over-forced-updates-and-unwanted-apps-18643135/>. [Kasutatud 02 04 2021].
- [5] C. Hoffman, „How-To Geek,“ 19 12 2019. [Võrgumaterjal]. Available: <https://www.howtogeek.com/442609/confirmed-windows-10-setup-now-prevents-local-account-creation/>. [Kasutatud 02 04 2021].
- [6] M. Brinkmann, „Microsoft may be collecting more data than initially,“ 01 05 2016. [Võrgumaterjal]. Available: <https://www.ghacks.net/2016/01/05/microsoft-may-be-collecting-more-data-than-initially-thought/>. [Kasutatud 03 04 2021].
- [7] “. P. Statement, 03 2021. [Võrgumaterjal]. Available: <https://privacy.microsoft.com/en-us/privacystatement>. [Kasutatud 03 04 2021].
- [8] M. Burnett, 21 05 2017. [Online]. Available: <https://twitter.com/m8burnett/status/866353982217699328>. [Accessed 04 04 2021].
- [9] M. Burnett, „Windows, Spying, and a Twitter Rant,“ 23 07 2017. [Võrgumaterjal]. Available: <https://xato.net/windows-spying-and-a-twitter-rant-19203babb2e7>. [Kasutatud 04 04 2021].
- [10] Pulse, „Как Windows следит за тобой. Как следит Linux. Тонкая настройка,“ 03 06 2019. [Võrgumaterjal]. Available: <https://hacker-basement.ru/2019/03/06/fine-tuning-windows-anonymity/>. [Kasutatud 05 04 2021].
- [11] Z. Whittaker, „Microsoft won't fix Windows flaw that lets hackers steal your,“ 02 08 2016. [Võrgumaterjal]. Available: <https://www.zdnet.com/article/windows-attack-can-steal-your-username-password-and-other-logins/>. [Kasutatud 04 04 2021].
- [12] B. Krebs, „At Least 30,000 U.S. Organizations Newly Hacked Via Holes in,“ 05 03 2021. [Võrgumaterjal]. Available: <https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/#comments>. [Kasutatud 06 04 2021].
- [13] J. Paul, „Your Computer Isn't Yours,“ 12 10 2020. [Võrgumaterjal]. Available: <https://sneak.berlin/20201112/your-computer-isnt-yours/>. [Kasutatud 06 04 2021].

- [14] Tails, „System requirements,“ [Võrgumaterjal]. Available: <https://tails.boum.org/doc/about/requirements/index.en.html>. [Kasutatud 05 04 2021].
- [15] K. Finley, „Out in the Open: Inside the Operating System Edward Snowden,“ 04 14 2014. [Võrgumaterjal]. Available: <https://www.wired.com/2014/04/tails/>. [Kasutatud 07 04 2021].
- [16] M. Lee, „What is free software?,“ 29 12 2009. [Võrgumaterjal]. Available: https://www.fsf.org/resources/what-is-fs/index_html. [Kasutatud 07 04 2021].
- [17] Gnu.org, „What is free software?,“ 03 02 2021. [Võrgumaterjal]. Available: <https://www.gnu.org/philosophy/free-sw>. [Kasutatud 07 04 2021].
- [18] Mozilla, "Firefox Privacy Notice," 01 03 2021. [Online]. Available: <https://www.mozilla.org/en-US/privacy/firefox/>. [Accessed 13 04 2021].
- [19] B. Bondy, „IPFS Support in Brave,“ 19 01 2021. [Võrgumaterjal]. Available: <https://brave.com/ipfs-support/>. [Kasutatud 13 04 2021].
- [20] G. Weinberg, „Why should I use DuckDuckGo instead of Google?,“ [Võrgumaterjal]. Available: <https://www.quora.com/Why-should-I-use-DuckDuckGo-instead-of-Google/answer/Gabriel-Weinberg>. [Kasutatud 18 04 2021].
- [21] A. Drozdov, „Linux Mint TalTech-i remix,“ 28 04 2021. [Võrgumaterjal]. Available: <https://gitlab.com/drozdovzx/linuxmint-taltech-remix>.
- [22] Ubuntu documentation, „LiveCDCustomization,“ [Võrgumaterjal]. Available: <https://help.ubuntu.com/community/LiveCDCustomization>. [Kasutatud 13 04 2021].
- [23] Longpanda, „Ventoy Main Page,“ 27 04 2021. [Võrgumaterjal]. Available: <https://ventoy.net/en/index.html>. [Kasutatud 27 04 2021].
- [24] A. Hern, „Microsoft productivity score feature criticised as workplace,“ 26 11 2020. [Võrgumaterjal]. Available: <https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance>. [Kasutatud 06 04 2021].
- [25] C. McAndrew, "Linux Privacy Essentials," 12 01 2015. [Online]. Available: <https://bit.ly/3eRYHkf>. [Accessed 09 04 2021].
- [26] G. Greenwald, "TEDGlobal 2014," 10 2014. [Online]. Available: https://www.ted.com/talks/glenn_greenwald_why_privacy_matters. [Accessed 01 04 2021].

Lisad

Lisa 1. Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks¹

Mina, Aleksandr Drozdov

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „TalTechi teadmiste võti – ülikooli digitaalne visiitkaart“, mille juhendaja on Edmund Laugasson
 - 1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
 - 1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

29.04.2021

¹ Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtjaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2. Skripti kood

```
#!/bin/bash

#-----
#---Prepare---
#-----

#Installing required packages and system updates
apt-get update
yes | apt-get install squashfs-tool
yes | apt-get install mkisofs

#Write here path to work directory, name for the new ISO-file and name of the default ISO-file
export WD="/home/alex/Desktop/ISO/"
export NEW_NAME="linuxmint-taltech-edition"
export OLD_NAME="linuxmint-20.1-cinnamon-64bit.iso"
cd $WD

#Removing the required directories if they are exist
rm -rf $WD/{edit,extract-cd,mnt,squashfs,squashfs-root}

#Mounting
mkdir mnt
mount -o loop $WD/$OLD_NAME mnt/

mkdir extract-cd
rsync --exclude=casper/filesystem.squashfs -a mnt/ extract-cd
unsquashfs mnt/casper/filesystem.squashfs

mkdir edit
mv squashfs-root/* edit
rm -rf squashfs-root

#You can use next method, which is a little faster, but there is no visual display of the loading bar
#mount -t squashfs -o loop mnt/casper/filesystem.squashfs squashfs
#cp -a squashfs/* edit/
#Bypass the restrictions on access to the file system that occur before the processes running in the chroot environment
mount --bind /dev edit/dev
```

Joonis 4. Paigaldused ja lahti pakkimine.

```
cat > edit/tmp/prepare.sh << ENDSRIPT
#!/bin/bash
mount -t proc none /proc
mount -t sysfs none /sys
mount -t devpts none /dev/pts
export HOME=/root
export LC_ALL=C.UTF-8
#configure connectivity
export NAMESERVER="8.8.8.8"
echo "nameserver ${NAMESERVER}" > /etc/resolv.conf
apt update
exit
ENDSCRIPT
```

Joonis 5. Chroot'i ettevalmistamine

```

cat > edit/tmp/custom.sh << ENDSRIPT
#!/bin/bash
yes | apt upgrade
#ID-card software
wget -O id.sh https://installer.id.ee/media/ubuntu/install-open-oid.sh
sed ':a;N;$!ba; s/test_root//2' id.sh > id-new.sh
yes | sh id-new.sh
rm id.sh id-new.sh

#Brave browser
apt-get update
yes | apt install apt-transport-https curl
curl -fsSLo /usr/share/keyrings/brave-browser-archive-keyring.gpg https://brave-browser-apt-release.s3.brave.com/brave-browser-archive-keyring.gpg
echo "deb [signed-by=/usr/share/keyrings/brave-browser-archive-keyring.gpg arch=amd64] https://brave-browser-apt-release.s3.brave.com/ stable main" |
sudo tee /etc/apt/sources.list.d/brave-browser-release.list
yes | apt update
yes | sudo apt install brave-browser

#Set Brave settings
wget https://gitlab.com/drozdovzx/linuxmint-taltech-remix/-/raw/master/BraveSoftware.zip -O /etc/skel/.config/BraveSoftware.zip
unzip /etc/skel/.config/BraveSoftware.zip -d /etc/skel/.config/
rm /etc/skel/.config/BraveSoftware.zip

```

Joonis 6. ISO muutused – ID-kaardi tarkvara, Brave veebilehitseja

```

#Set incognito by default
mkdir /etc/skel/.local/share/applications/
cp /usr/share/applications/brave-browser.desktop /etc/skel/.local/share/applications/brave-browser.desktop
sed -i 's/brave-browser-stable/brave-browser-stable --incognito --password-store=basic/g' /etc/skel/.local/share/applications/brave-browser.desktop
sed -i 's/--incognito --password-store=basic --incognito --incognito --password-store=basic/g' /etc/skel/.local/share/applications/brave-browser.desktop

#Clear clipboard every 1 min
yes | sudo apt install xclip
cat > etc/skel/.local/clipboard.sh <<EOF
#!/bin/bash
xsel -bc
xsel -x -bc
xsel -x
xclip < /dev/null
EOF
chmod +x etc/skel/.local/clipboard.sh
chmod -w etc/skel/.local/clipboard.sh
(crontab -l 2>/dev/null; echo "* * * * * etc/skel/.local/clipboard.sh") | crontab -

```

Joonis 7. ISO muutused – tundmatu režiim vaikimisi, lõikepuhvri kustutamine

```

#Other
sudo wget -O /usr/share/backgrounds/linuxmint/default_background.jpg https://portal-int.taltech.ee/sites/default/files/styles/manual_crop/public/news-image/TalTech_Zoom_tautst_1920x1080px-09_0.jpg?itok=j0S5GA_7
yes | apt-get purge thunderbird*
yes | apt-get purge pidgin*
yes | apt-get purge gimp*
yes | sudo apt-get purge firefox
rm -rf ~/.mozilla
yes | apt-get upgrade
exit
ENDSCRIPT

```

Joonis 8. ISO muutused - taustapilt ja puhastamine

```

chmod +x edit/tmp/*.sh
chroot edit ./tmp/prepare.sh
#If you want to test something in the chroot environment, then uncomment next strings
#chroot edit
#exit

chroot edit ./tmp/custom.sh
chroot edit ./tmp/cleanup.sh
umount edit/dev

```

Joonis 9. Chroot'i käivitamine

```
#Manifest file
chmod +w extract-cd/casper/filesystem.manifest
chroot edit dpkg-query -W --showformat='${Package} ${Version}\n' > extract-cd/casper/filesystem.manifest
chmod -w extract-cd/casper/filesystem.manifest
```

Joonis 10. Manifest faili muutus

```
rm -f $WD/extract-cd/casper/filesystem.squashfs
#Default block size is 131072 bytes
mksquashfs $WD/edit $WD/extract-cd/casper/filesystem.squashfs
#Highest possible compression but it takes much more time
#mksquashfs edit extract-cd/casper/filesystem.squashfs -comp xz -e edit/boot
```

Joonis 11. Vana failisüsteemi kustutamine ja uue failisüsteemi pakkimine

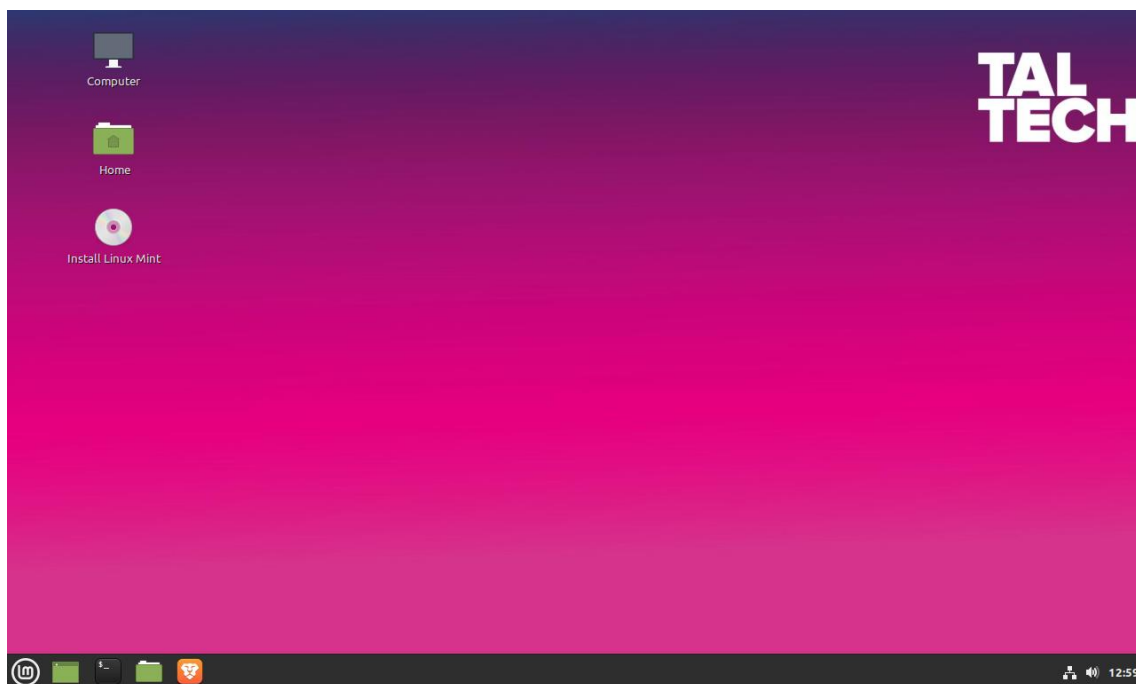
```
#Generate customized ISO-file
mkisofs -D -r -V "$NEW_NAME" -cache-inodes -J -l -b isolinux/isolinux.bin -c isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -o .
./$NEW_NAME.iso .

#---Checksum generating---
cd ../
sha256sum $NEW_NAME.iso > $NEW_NAME.iso.sha256
sha256sum -c $NEW_NAME.iso.sha256
```

Joonis 12. Uue ISO-faili ja kontrollsumma loomine

```
#---Unmount and delete directories---
umount edit/dev
umount edit/run
umount edit/proc
umount edit/sys
umount mnt
rm -rf extract-cd
rm -rf mnt
rm -rf edit
```

Joonis 13. Puhastamine



Joonis 14. Modifitseeritud OSi töölaud