

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\Disk Software\Microsoft\Windows NT\CurrentVersion

Computer

HKEY\_CLASSES\_ROOT

HKEY\_CURRENT\_USER

HKEY\_LOCAL\_MACHINE

BCD00000000

Disk Software

7-Zip

Classes

Clients

Google

Intel

Macromedia

Microsoft

.NETFramework

AccountsControl

Active Setup

ActiveSync

ADs

Advanced INF Setup

ALG

AllUserInstallAgent

AMSI

Analog

AppServiceProtocols

AppV

AppVISV

Assistance

AuthHost

BidInterface

BitLockerCsp

CallAndMessagingEnhancement

Cellular

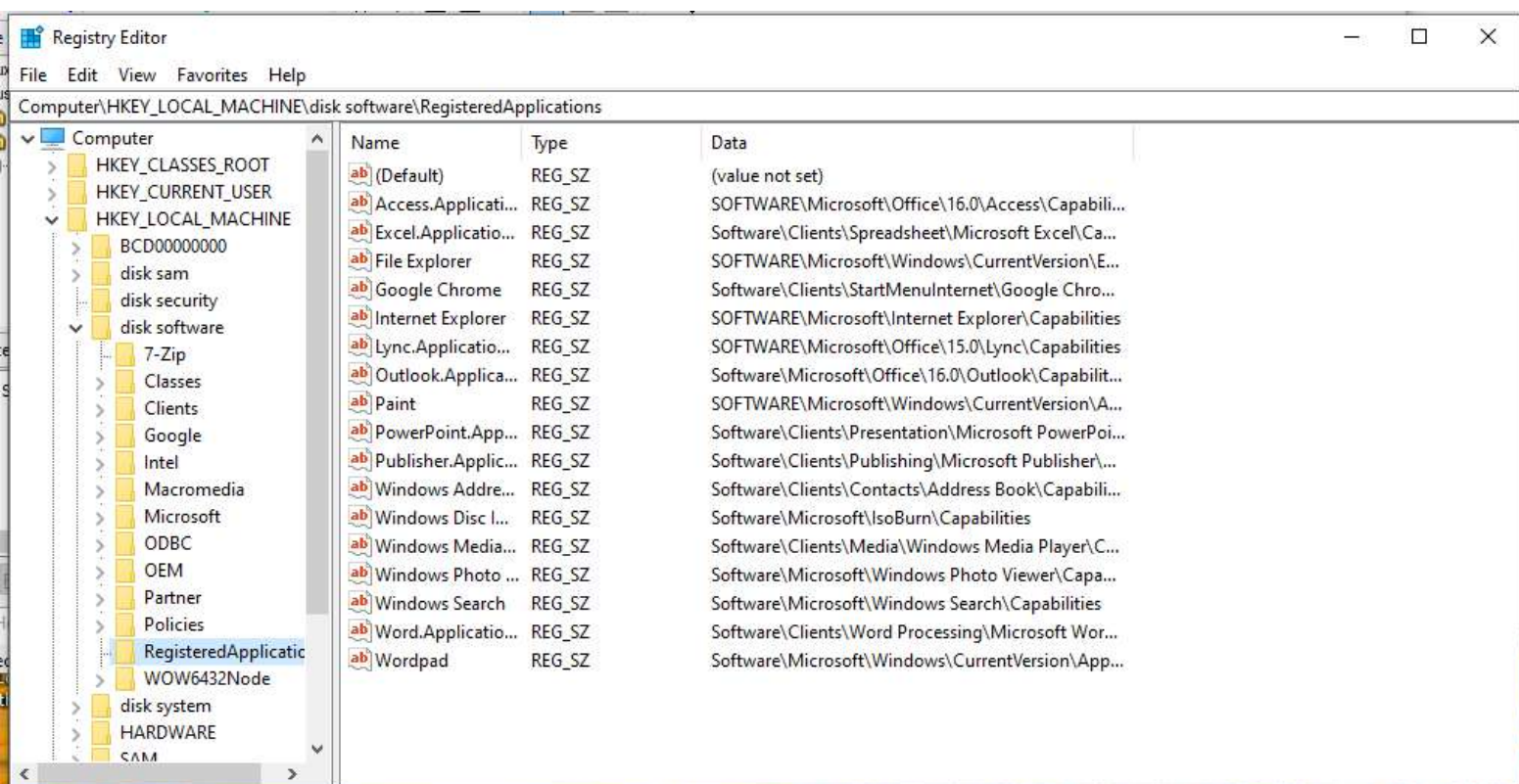
Chkdsk

ClipboardServer

COM3

Command Processor

Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildBranch	REG_SZ	rs3_release
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffffffff
BuildLab	REG_SZ	16299.rs3_release.170928-1534
BuildLabEx	REG_SZ	16299.15.amd64fre.rs3_release.170928-1534
CompositionEdi...	REG_SZ	Professional
CurrentBuild	REG_SZ	16299
CurrentBuildNu...	REG_SZ	16299
CurrentMajorVer...	REG_DWORD	0x0000000a (10)
CurrentMinorVe...	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 33 33 31 2d 31 30 30 3...
DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 30 00 30 00 30 00 30 00 00...
EditionID	REG_SZ	Professional
EditionSubstring	REG_SZ	
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x5c4cb089 (1548529801)
InstallTime	REG_QWORD	0x1d4b5aabc6a002e (131930034010718254)
PathName	REG_SZ	C:\Windows
ProductId	REG_SZ	00331-10000-00001-AA821
ProductName	REG_SZ	Windows 10 Pro
RegisteredOrga...	REG_SZ	
RegisteredOwner	REG_SZ	Windows User
ReleaseId	REG_SZ	1709
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\Windows
UBR	REG_DWORD	0x00000040 (64)



Kernel OST Viewer

FILE VIEW FIND HELP

Select File Find ? Help

Folder List

- Common Views
- Drizzle
- Finder
- IPM\_SUBTREE
- Archive
- Calendar
- Birthdays
- United States I
- Contacts
- (08967759-274D)
- (A9E28C46-B3A)
- Companies
- GAL Contacts
- Organizational I
- PeopleCentricC
- Recipient Cach
- Conversation Actio
- Conversation Histo
- Team Chat
- Deleted Items
- Drafts
- ExternalContacts
- Files
- Inbox
- Journal
- Junk Email
- Notes
- Outbox
- PersonMetadata
- Quick Step Settings
- Recent

Inbox (36)

	From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>	<FILTER>
	Alpaca Activists<aausa@gmail.com>	Re: Interested in the job	Sun 03/17/2019 07:19 AM	Existing
	Alpaca Activists<aausa@gmail.com>	Re: Interested in the job	Sun 03/17/2019 07:44 AM	Existing
	jeff astrologo<deea7ab4f62...>	Re: Job Needed, 19709	Sun 03/17/2019 12:20 PM	Existing
	Jaehua Tetraut<8f96e880df...>	Re: I saw your add!	Sun 03/17/2019 12:35 PM	Existing
	Alpaca Activists<aausa@gmail.com>	Re: Interested in the job	Fri 03/22/2019 02:47 AM	Existing
	Alpaca Activists<aausa@gmail.com>	Re: Interested in the job	Fri 03/22/2019 02:55 AM	Existing
	Karen Alice<klovespizza@outlook.com>	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Existing
	Karen Alice<klovespizza@outlook.com>	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Lost/Deleted
	craigslat reply 5dde<5dde4b...>	Job Needed, 19709	Tue 02/19/2019 07:16 AM	Lost/Deleted
	Jeff Astrologo<deea7ab4f62...>	Job Needed, 19709	Wed 02/13/2019 13:27 PM	Lost/Deleted

Simple View Advanced Properties View

**Re: Interested in the job**  
Alpaca Activists<aausa@gmail.com> Fri 03/22/2019 02:55 AM  
To: "Karen Alice" <klovespizza@outlook.com>

**Links:**

- <https://null-byte.wonderhowto.com/how-to/essential-skills-becoming-master-hacker-0154509/>
- <https://www.torproject.org/about/overview.html.en>

- For this link, learn what Tor is, and how to set it up

File Analysis Reports

- Total item types
- Mail flow density by date
- Mail flow density by senders
- Interaction between users



Evidence Tree

- User Data
  - BrowserMetrics
  - CertificateRevocation
  - CertificateTransparen
  - Crashpad
  - Default
  - FileTypePolicies
  - InterventionPolicyDat
  - MEIPreload
  - OriginTrials
  - PepperFlash
  - pnacI
  - SafeBrowsing
  - ShaderCache
  - SSLErrorAssistant
  - SubresourceFilter
  - SwReporter

File List

Name	Size	Type	Date Accessed	Date Created	Date Modified
\$I30	4,096 (4 KB)	NTFS Index All...	3/22/2019 11:23:58 PM	2/9/2019 8:29:51 PM	3/22/2019 11:23:58 PM
CertCsdDownloadWhitelist.store	1,305 (2 KB)	Regular File	3/13/2019 4:39:32 AM	3/13/2019 4:39:32 AM	3/13/2019 4:39:32 AM
CertCsdDownloadWhitelist.store.FileSlack	2,791 (3 KB)	File Slack			
ChromeExtMalware.store	801,726 (783 KB)	Regular File	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM
ChromeExtMalware.store.FileSlack	1,090 (2 KB)	File Slack			
ChromeUrlClientIncident.store	729 (1 KB)	Regular File	3/13/2019 4:39:32 AM	3/13/2019 4:39:32 AM	3/13/2019 4:39:32 AM
ChromeUrlClientIncident.store.FileSlack	3,367 (4 KB)	File Slack			
IpMalware.store	106 (1 KB)	Regular File	3/13/2019 4:39:30 AM	3/13/2019 4:39:30 AM	3/13/2019 4:39:31 AM
UrlBilling.store	821 (1 KB)	Regular File	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM
UrlCsdDownloadWhitelist.store	32,989 (33 KB)	Regular File	3/21/2019 7:20:58 PM	3/21/2019 7:20:58 PM	3/21/2019 7:20:58 PM
UrlCsdWhitelist.store	4,515 (5 KB)	Regular File	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM
UrlCsdWhitelist.store.FileSlack	3,677 (4 KB)	File Slack			
UrlMalBin.store	103,095 (101 KB)	Regular File	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM	3/22/2019 11:23:58 PM

Custom Content Sources

Evidence:File System|Path|File Options

Empty area for custom content sources.

New Edit Remove Remove All Create Image



8226266af9a324badf0af79158f115fa5b35ca673f1ca8679c6e0e8051b981a0

8226266af9a324badf0af79158f115fa5b35ca673f1ca8679c6e0e8051b981a0

36/72 security vendors flagged this file as malicious

ReanalyzeSimilarMore

36/72

Community Score -1

8226266af9a324badf0af79158f115fa5b35ca673f1ca8679c6e0e8051b981a0

antimalwaresetup.exe

Size861.99 KB

Last Analysis Date29 days ago

EXE

peexe direct-cpu-clock-access runtime-modules corrupt idle overlay upx

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.safebytes/plumbytes

Threat categoriestrojanadwarepua

Family labelssafebytesplumbytesunwantedx

Security vendors' analysis

Do you want to automate checks?

AliCloud	Trojan:Win/SafeBytes.A	Antiy-AVL	GrayWare/Win32.SafeBytes
Arcabit	Trojan.Generic	Arctic Wolf	Unsafe
Avast	Win32:UnwantedX-gen [PUP]	AVG	Win32:UnwantedX-gen [PUP]
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/grayware_confidence_100% (W)

C:\Users\<USER>\Desktop\program.exe

#### Registry actions

##### Registry Keys Opened

- HKEY\_CURRENT\_USER\Software\Borland\Delphi\Locales
- HKEY\_CURRENT\_USER\Software\Borland\Locales
- HKEY\_CURRENT\_USER\Software\CodeGear\Locales
- HKEY\_CURRENT\_USER\Software\Embarcadero\Locales
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\input\MaxResyncAttempts
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\input\ResyncResetTime
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE

#### Process and service actions

Registry Editor

File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\disk software\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink

ClipSVC

Compatibility32

Console

CorruptedFileRecove

DefaultProductKey

DeviceDisplayObject

DiskDiagnostics

drivers.desc

Drivers32

EFS

EMDMgmt

Event Viewer

Font Drivers

Font Management

FontDPI

FontIntensityCorrecti

FontLink

SystemLink

FontMapper

FontMapperFamilyFa

Fonts

FontSubstitutes

GRE\_Initialize

HostActivityManager

ICM

Image File Execution

IniFileMapping

KnownFunctionTable

KnownManagedDebu

LanguagePack

LicensingDiag

MCI Extensions

MCI32

MiniDumpAuxiliaryD

MsiCorruptedFileRec

Multimedia

Name	Type	Data
(Default)	REG_SZ	(value not set)
Batang	REG_MULTI_SZ	MSMINCHO.TTC,MS PMincho MINGLIU.TTC,PMin...
BatangChe	REG_MULTI_SZ	MSMINCHO.TTC,MS Mincho MINGLIU.TTC,MingLi...
Dotum	REG_MULTI_SZ	MSGOTHIC.TTC,MS UI Gothic MINGLIU.TTC,PMing...
DotumChe	REG_MULTI_SZ	MSGOTHIC.TTC,MS Gothic MINGLIU.TTC,MingLiU ...
Ebrima	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Ebrima Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Gadugi	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Gadugi Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Gulim	REG_MULTI_SZ	MICROSS.TTF,Microsoft Sans Serif,128,140 MICROS...
GulimChe	REG_MULTI_SZ	MSGOTHIC.TTC,MS Gothic MINGLIU.TTC,MingLiU ...
Gungsuh	REG_MULTI_SZ	MSMINCHO.TTC,MS PMincho MINGLIU.TTC,PMin...
GungsuhChe	REG_MULTI_SZ	MSMINCHO.TTC,MS Mincho MINGLIU.TTC,MingLi...
Khmer UI	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Khmer UI Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Lao UI	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Lao UI Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Leelawadee	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Leelawadee Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Leelawadee UI	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,110,82 SEGOEUI.TTF,Segoe ...
Leelawadee UI B...	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,110,82 SEGOEUIB.TTF,...
Lucida Sans Uni...	REG_MULTI_SZ	MSGOTHIC.TTC,MS UI Gothic MINGLIU.TTC,PMing...
Malgun Gothic	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,130,81 SEGOEUI.TTF,Segoe ...
Malgun Gothic ...	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,130,81 SEGOEUIB.TTF,...
Malgun Gothic ...	REG_MULTI_SZ	SEGOEUISL.TTF,Segoe UI Semilight,130,81 SEGOEUI...
Meiryo	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,133,83 SEGOEUI.TTF,Segoe ...
Meiryo Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,133,83 SEGOEUIB.TTF,...
Meiryo UI	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,133,83 SEGOEUI.TTF,Segoe ...
Meiryo UI Bold	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,133,83 SEGOEUIB.TTF,...
Microsoft Jheng...	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,114,78 SEGOEUI.TTF,Segoe ...
Microsoft Jheng...	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,114,78 SEGOEUIB.TTF,...
Microsoft Jheng...	REG_MULTI_SZ	SEGOEUI.TTF,Segoe UI,114,78 SEGOEUI.TTF,Segoe ...
Microsoft Jheng...	REG_MULTI_SZ	SEGOEUIB.TTF,Segoe UI Bold,114,78 SEGOEUIB.TTF,...

Kernel OST Viewer

FILEVIEWFINDHELP

Select FileFindHelp

Folder List

Common Views

Drizzle

Finder

IPM\_SUBTREE

Archive

Calendar

Birthdays

United States I

Contacts

{06957759-274D

{A9E2BC46-B3A

Companies

GAL Contacts

Organizational

PeopleCentricC

Recipient Cach

Conversation Actio

Conversation Histo

Team Chat

Deleted Items

Drafts

ExternalContacts

Files

Inbox

Journal

Junk Email

Notes

Outbox

PersonMetadata

Quick Step Settings

Inbox (35)

From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 07:19 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 07:44 AM	Existing
jeff astrologo<deea7ab4f62...	Re: Job Needed, 19709	Sun 03/17/2019 12:20 PM	Existing
Jashua Tetrault<8f95e860df...	Re: I saw your add!	Sun 03/17/2019 12:35 PM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 02:47 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 02:55 AM	Existing
Karen Alice<klovespiz@o...	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Existing
Karen Alice<klovespiz@o...	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Lost/Deleted
craigslst reply 5dde<5dde4b...	Job Needed, 19709	Tue 02/19/2019 07:16 AM	Lost/Deleted
Jeff Astrologo<deea7ab4f62...	Job Needed, 19709	Wed 02/13/2019 13:27 PM	Lost/Deleted

Simple View

Advanced Properties View

RE: Interested in the job

Karen Alice<klovespiz@outlook.com>

Sat 03/23/2019 00:37 AM

To: "Karen Alice" <klovespiz@outlook.com>

Attachments: Skype Convo.zip

MS

Things didn't go as planned with Bob. I attached a copy of our chat history. The password is **pacalove**

From: Karen Alice

Sent: 22 March 2019 01:53

To: 'Alpaca Activists' <taausai@gmail.com>

Subject: RE: Interested in the job

File Analysis Reports

Total item types

Mail flow density by date

Mail flow density by senders

Interaction between users

Karen, 19:45 (wave)

Bob, 19:46  
Howdy

Karen, 19:46  
OMG I'm so happy you answered!

Bob, 19:46  
Why?

Karen, 19:46  
I love people that love Alpacas!

Bob, 19:46  
Oh wow. Me too!

Karen, 19:47  
Although, I must inform you, your profile pic is a llama not a paca baby

Bob, 19:47  
Yeah, I know. Its a test. I have to weed out the fakers.

Karen, 19:47  
Oh I feel that.

Karen, 19:48

<

Inbox ( 36 )

From	Subject	Date/Time	Lost/Deleted
<FILTER>	<FILTER>	<FILTER>	<FILTER>
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 07:19 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Sun 03/17/2019 07:44 AM	Existing
jeff astrologo<deea7ab4f62...	Re: Job Needed, 19709	Sun 03/17/2019 12:20 PM	Existing
Jashua Tetrault<6f96e860df...	Re: I saw your add!	Sun 03/17/2019 12:35 PM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 02:47 AM	Existing
Alpaca Activists<taausai@g...	Re: Interested in the job	Fri 03/22/2019 02:55 AM	Existing
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Existing
Karen Alice<klovespizza@o...	RE: Interested in the job	Sat 03/23/2019 00:37 AM	Lost/Deleted
craigslist reply 5dde<5dde4b...	Job Needed, 19709	Tue 02/19/2019 07:16 AM	Lost/Deleted
Jeff Astrologo<deea7ab4f62...	Job Needed, 19709	Wed 02/13/2019 13:27 PM	Lost/Deleted

Simple View Advanced Properties View

**RE: Interested in the job**  
 Karen Alice<klovespizza@outlook.com>  
 To: "Karen Alice" <klovespizza@outlook.com>  
 Attachments: Skype Convo.zip  
 Sat 03/23/2019 00:37 AM

mistreating some of his Alpacas. We have heard complaints that he refuses to provide Alpacas with scarfs and beanies during the winter!

What we need you to do is gain his trust and then hack his machine. We will give you more information about this in person. Meet us here "27°22'50.10"N, 33°37'54.62"E"

On Sun, Mar 17, 2019 at 2:48 AM Karen Alice <klovespizza@outlook.com> wrote:

Hi Michael,

I've always been interested in this kind of work (more in the hacking side) but never got around to learning about it. I think this will be an awesome opportunity for me to learn more and maybe even protect my own computer from hackers!

27°22'50.1"N 33°37'54.6"E

27°22'50.1"N 33°37'54.6"E

27.380583, 33.631639

Directions

Save

Nearby

Send to phone

Share

9JJJ+6PP Hurghada 2, Egypt

Add a missing place

Add your business

Add a label

Your Maps activity

