ACM NetSec

Cybersecurity Made Simple

Personal Security

ACM NetSec, Fall 2017

Agenda

- Intro to NetSec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

ACM NetSec

Cybersecurity Made Simple

What is NetSec?

- “Cybersecurity made simple”
- Plans for this year:
  - Tracks
  - Community
  - Capture the Flag competition
- CTF!!

What is a “track” ?

A track is a 5 week workshop series taught about a particular topic

Tracks this quarter:

Personal Security: Learn about security threats and how to protect yourself in the digital age

Web Hacking: Learn about cybersecurity threats and exploits plaguing web applications and how you can defend against them

CTF: Learn how to tackle CTF problems and compete in CTFs together

Tracks

Personal Security
Time: 7:00PM - 9:00PM, Monday 10/9 (Week 2)
Location: ACM Clubhouse

Web Hacking
Time: 7:00PM - 9:00PM, Tuesday 10/17 (Week 3)
Location: ACM Clubhouse

Capture the Flag
Time: 7:00PM -9:00PM, Thursday 10/26 (Week 4)
Location: ACM Clubhouse

Agenda

- Intro to Netsec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

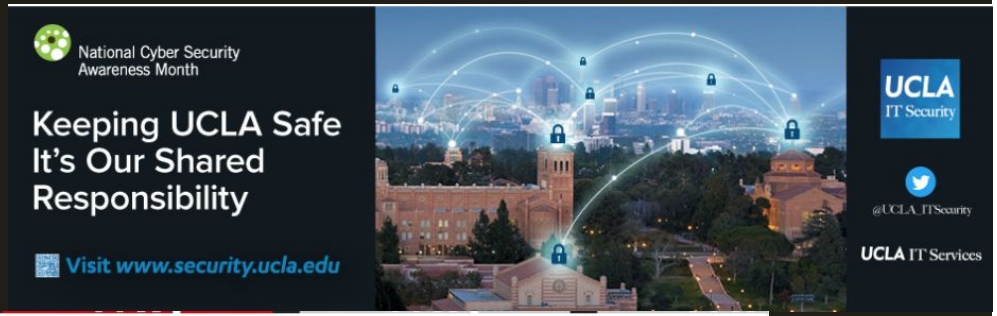
The Five Why's

Why Why Why Why Why

Why am I coming to the Personal Security track?

Because I want to learn about **cybersecurity**.

Why Why Why Why Why



> *We have witnessed an increase of 82% in cyber crimes rates in the United States over the last six years.*

Why Why Why Why Why

Why do I want to learn about cybersecurity?

Because I want to **protect myself** on the Internet.

Why Why Why Why Why

Protect Yourself With a Free VPN Service

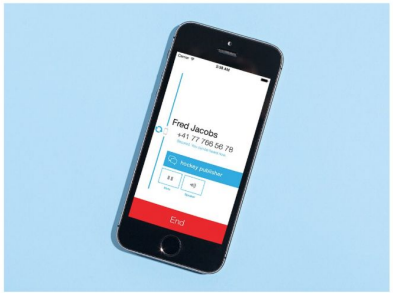
Can't afford a premium VPN? That's no reason to leave your network traffic unprotected. Here's everything you need to know about free VPN services.

By Max Eddy July 10, 2017 3:57PM EST

765 SHARES

ANDY GREENBERG SECURITY 07.29.14 01:30 AM

YOUR IPHONE CAN FINALLY MAKE FREE, ENCRYPTED CALLS



The encrypted calling app Signal. The two seemingly random words beneath the contact's name are meant to be read out at the beginning of a conversation to make sure no man-in-the-middle snoop has eavesdropped on the call. WIRED

SECURITY

Two-factor authentication: What you need to know (FAQ)

Twitter's got it. Apple's got it, too. Google, Microsoft, Facebook and Amazon have had it for a while. But why's two-factor authentication important, and will it keep you safe?

BY SETH ROSENBLATT, JASON CIPRIANI / JUNE 15, 2015 1:39 PM PDT

Why do I want to protect myself on the internet?

Because I don’t want a malicious individual to **hack** me.

Why Why Why Why Why

More Than 120,000 Internet Connected Cameras Can Be Easily Hacked, Researcher Warns

Oh, Internet of Things.

SHARE TWEET

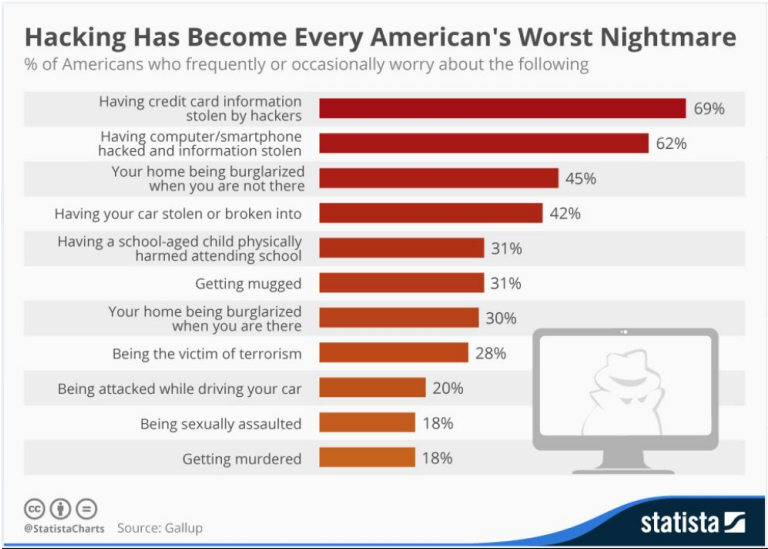
Cyber-Safe

Cybercrime costs the average U.S. firm $15 million a year

by James Griffiths @CNNTech

October 8, 2015: 3:28 AM ET

2. The Hackable Cardiac Devices from St. Jude



Why don’t I want to be hacked?

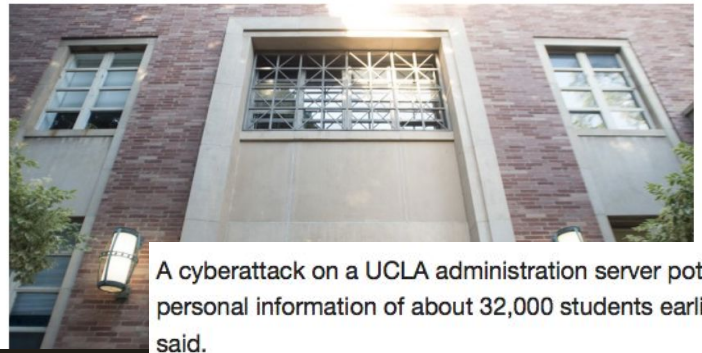
Because I have a lot of personal information online that should remain **private**.

Why Why Why Why Why

Cyberattack on UCLA server potentially accesses student information

BY JACOB PREAL
Posted: August 4, 2017 1:53 pm

CAMPUS, CRIME, NEWS



A cyberattack on a UCLA administration server potentially breached the personal information of about 32,000 students earlier this week, UCLA officials said.

POLICY —

Police ask: "Alexa, did you witness a murder?"

Drowning in hot tub was followed by 140-gallon hose-down recorded by utility.

SEAN GALLAGHER - 12/28/2016, 12:45 PM

TECHNOLOGY

Breaking Down Apple's iPhone Fight With the U.S. Government

By THE NEW YORK TIMES UPDATED March 21, 2016

Why should my personal information remain private?

Because my personal information gives me access to my **money**, my **personal contacts**, my **identification**, and I don't want that to be taken advantage of.

Why Why Why Why Why

Cedars-Sinai says number of patient files in data breach much higher

BUSINESS

Equifax Breach Exposes Personal Data Of 143 Million People

September 8, 2017 · 4:30 PM ET

Heard on All Things Considered

San Francisco sues Equifax on behalf of 15 million Californians affected by the breach

Posted Sep 27, 2017 by Sarah Buhr (@sarahbuhr)

Agenda

- Intro to Netsec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

CIA Principle

Confidentiality

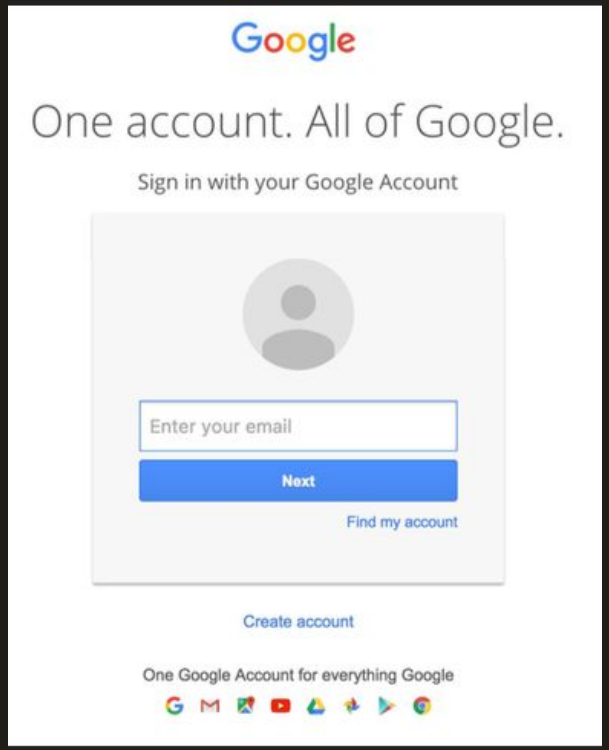
Integrity

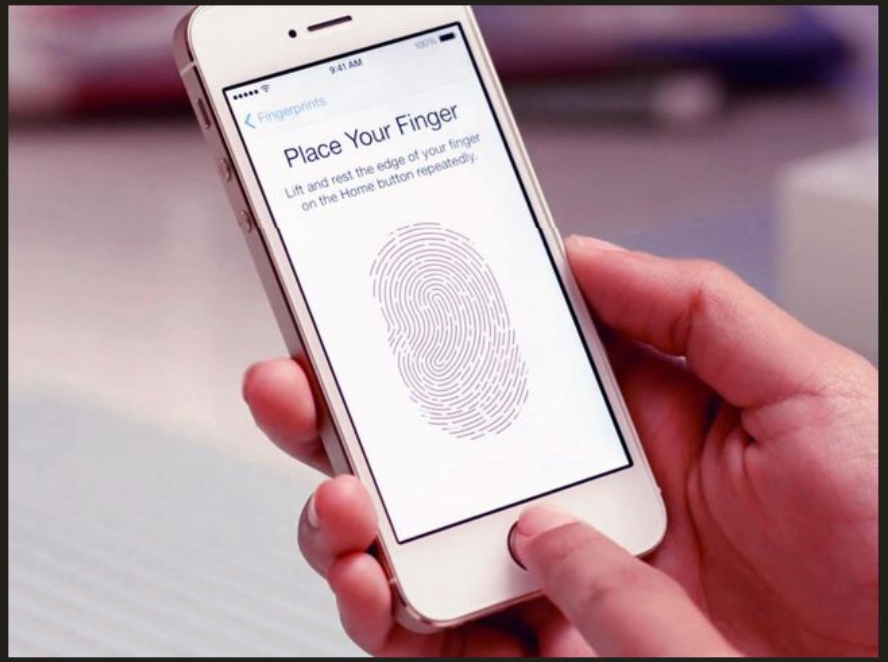
Accessibility

Confidentiality

Confidentiality:

Ability to hide information from those people unauthorized to view it


Google
One account. All of Google.
Sign in with your Google Account
Enter your email
Next
Find my account
Create account
One Google Account for everything Google


9:41 AM
Fingerprints
Place Your Finger
Lift and rest the edge of your finger on the Home button repeatedly.

Integrity

Integrity:

Ability to ensure that data is an accurate and unchanged representation of the original secure information


Software update
"Mac Media Player" is out of date
The version of "Mac Media Player" on your system does not include the latest security updates and has been blocked. To continue using "Mac Media Player", download an updated version.
Download Media...
OK
The new version of Mac Media Player is ready to download.
DOWNLOAD

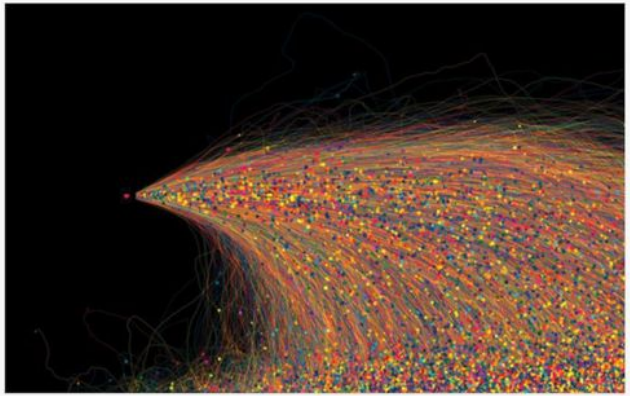
Availability

Availability:

Ability to ensure that the information concerned is readily accessible to the authorized viewer at all times

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Posted Oct 21, 2016 by Darrell Etherington (@etherington), Kate Conger (@kateconger)



Several waves of major cyberattacks against an internet directory service knocked dozens of popular websites offline today, with outages continuing into the afternoon.

Twitter, SoundCloud, Spotify, Shopify, and other websites have been inaccessible to many users throughout the day. The outages are the result of several distributed denial of service

Crunchbase

Twitter –

FOUNDED
2006

OVERVIEW
Twitter is a global social networking platform that allows its users to send and read 140-character messages known as "tweets". It enables registered users to read and post their tweets through the web, short message service (SMS), and mobile applications. As a global real-time communications platform, Twitter has more than 400 million monthly visitors and 255 million monthly active users around ...

LOCATION
San Francisco, CA

CATEGORIES
SMS, Blogging Platforms, Social Media, Messaging

WEBSITE
http://www.twitter.com/

Full profile for Twitter

Spotify +

Issues and Alternatives

- Parkerian Hexad - CIA extension
  - Confidentiality
  - Possession or Control
    - Stolen card
  - Integrity
  - Authenticity
    - Signing a message
  - Availability
  - Utility
    - Bad data format

- STRIDE
  - Spoofing of user identity
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service (D.o.S)
  - Elevation of privilege
- DREAD
  - You get the idea - lots of acronyms

Agenda

- Intro to Netsec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

What does “hack” mean?


Hack?
Def: Maliciously taking advantage of a system's CIA paradigms

Hack?

ACM Hack

hackschool

LEARN SESSION

WEEK 1

Intro to Web Development

Def: A slang for innovatively solving a problem or making a product

Hackathon?

Def: Programming competitions where students are encouraged to build anything they'd like

What does “hack” mean?

Agenda

- Intro to Netsec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

Hacking in Pop Culture

Misrepresentation

CULTURE

CNN uses Fallout 4 screenshot in report on Russian hacking

Russian hackers most likely did not use Pip-Boys to disrupt the US presidential election.

BY **ALFRED NG** / JANUARY 3, 2017 6:55 AM PST

CNN used this shot of Fallout 4 to show what hacking looks like.

CNN (Screenshot by Alfred Ng/CNET)

Fallout 4 features a hacking mini-game.

YouTube (Screenshot by Alfred Ng/CNET)

https://www.cnet.com/news/cnn-uses-fallout-4-screenshot-in-report-on-russian-hacking/

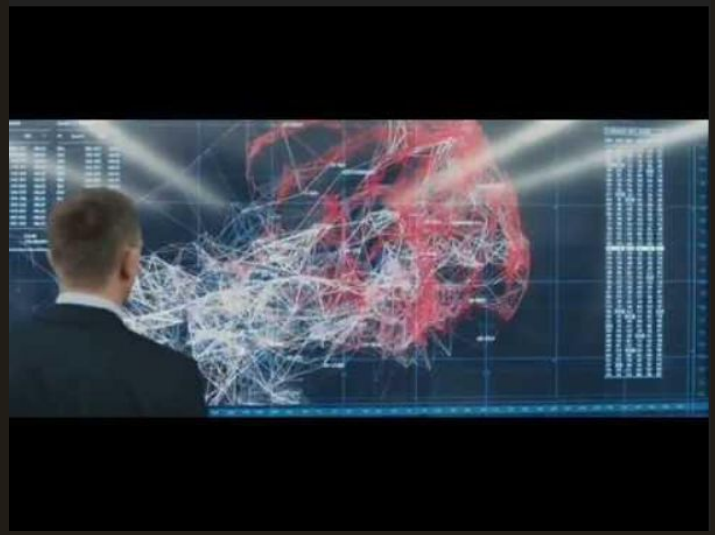
The Ugly: 90s Computer Hacking Supercut

https://www.youtube.com/watch?v=bbOEHcA-71I&feature=youtu.be

What was ugly about that?

- Cheesy lines
- Horrible/unrealistic CGI
- Black box hacking process
- Poor plot-driving method

The Bad: Skyfall



https://www.youtube.com/watch?v=aApTVqeGJMw

What was bad about that?

- Elaborate Graphical Interface
- “What if you try this” cliche
- Unrealistic decryption
- “They hacked us”/ “I’m in” cliche

The Good

https://www.youtube.com/watch?v=g6gG-6Co_v4

What was good about that?

- Clear explanation of vulnerability
- Clear motivation for hacking
- Realistic props and computer scenes

MR. ROBOT VS SKYFALL

- Simple Dialogue
- Real computer interface
- Current-world

- Complex Back-and-Forth
- Futuristic machine
- Fiction

[case] Hospital Hacking

- $3.6 million in Bitcoin
- “The fact that hackers were able to encrypt patient records doesn't necessarily mean they gained access to those files, but the goal of this type of cyberattack isn’t to get to patient information; it’s to make sure that the hospital can’t get to it, either.”

- Known as ransomware

A Hospital Paralyzed by Hackers

A cyberattack in Los Angeles has left doctors locked out of patient records for more than a week. Unless the medical facility pays a ransom, it’s unclear that they'll get that information back.

KAVEH WADDELL | FEB 17, 2016 | TECHNOLOGY

Share Tweet ...

TEXT SIZE – +

Like *The Atlantic*? Subscribe to The Atlantic Daily, our free weekday email newsletter. Email SIGN UP

A hospital in Los Angeles has been operating without access to email or electronic health records for more than a week, after hackers took over its computer systems and demanded millions of dollars in ransom to return it.

The hackers that broke into the Hollywood Presbyterian Medical Center’s servers are asking for $3.6 million in Bitcoin, a local Fox News affiliate reported. Hospital staff are working with investigators from the Los Angeles Police Department and the FBI to find the intruders’ identities.

Even Worse?

https://www.youtube.com/watch?v=K7Hn1rPQouU

Agenda

- Intro to Netsec
- Why Cybersecurity?
- CIA Principle
- “Hack”
- Hacking in Pop Culture
- PGP/GPG
- Practical file encryption (no need to install any software!)

PGP/GPG

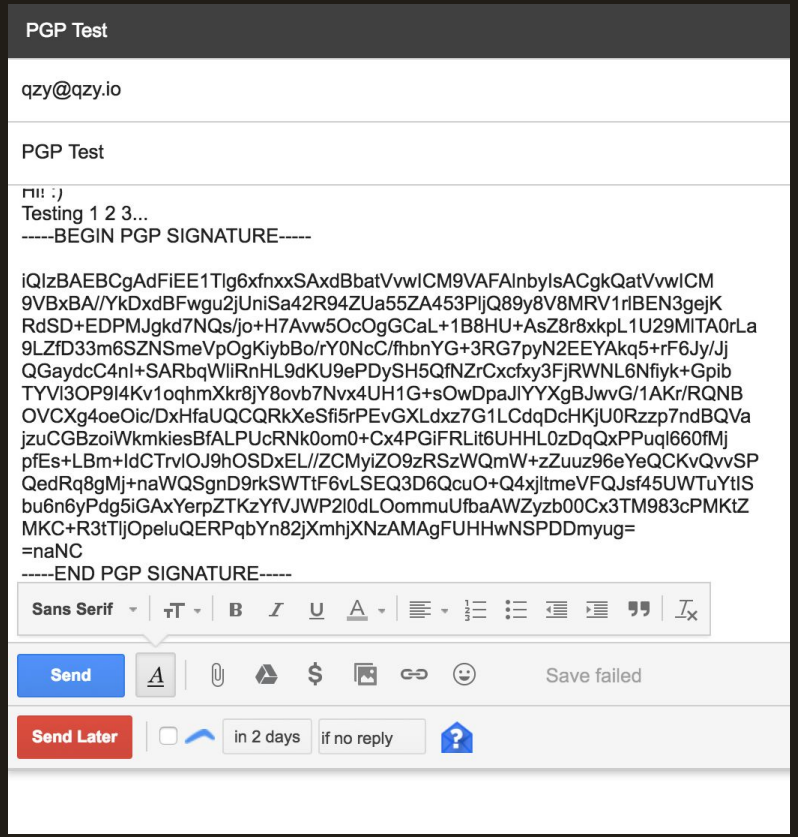
- Intro to confidentiality
- PGP = Pretty Good Privacy
- GPG = Gnu Privacy Guard
  - Implementation of PGP standards
- More resources
  - https://ssd.eff.org/
  - http://notes.jerzygangi.com/the-best-pgp-tutorial-for-mac-os-x-ever/

PGP/GPG

- Install GPG Suite
  - https://gpgtools.org/
- Open GPG Keychain
  - Generate Key
  - Use complex password!
- System Preferences » Keyboard » Shortcuts
- Set shortcuts
  - Decrypt: ^⌥⌘-
  - Encrypt: ^⌥⌘=
  - Sign: ^⌥⌘[
  - Verify: ^⌥⌘]

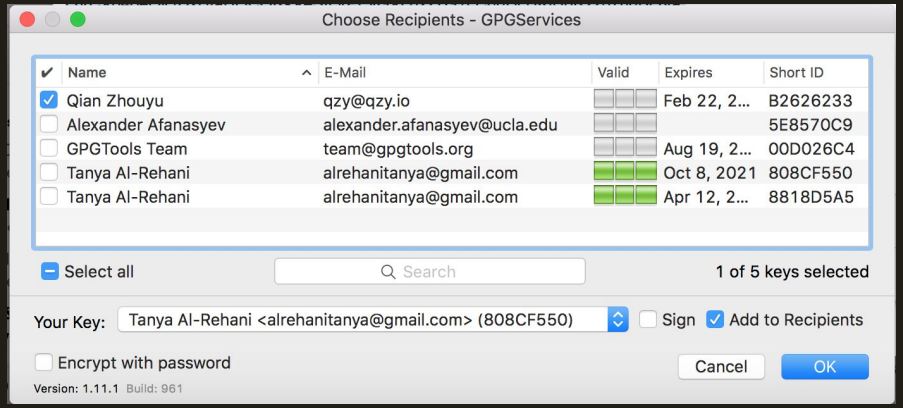
PGP/GPG - Cont.

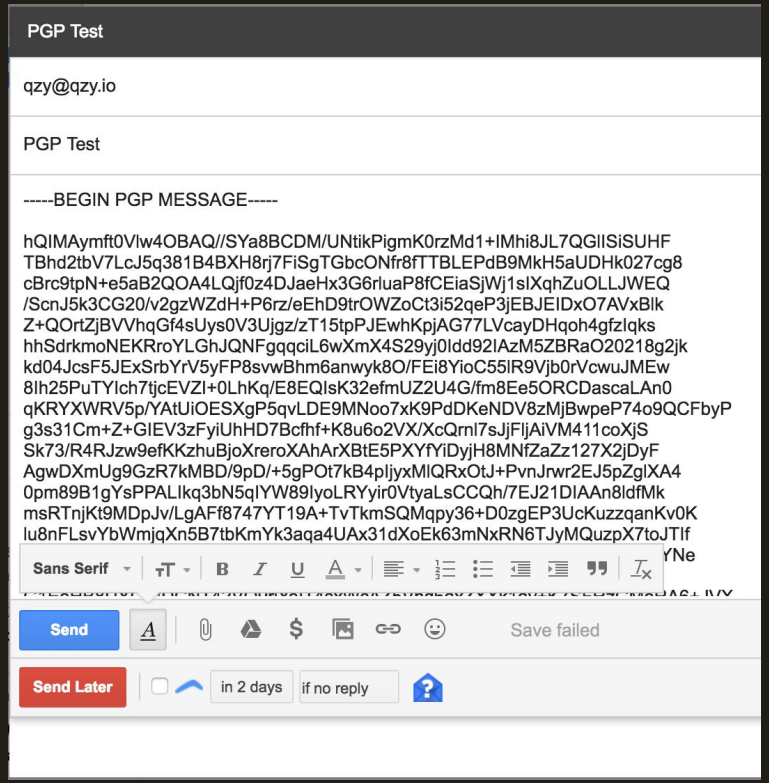
- Use a keyserver to look up public keys
- New Email
  - Send to: alrehanitanya@gmail.com
  - Type message
  - Ctrl-Click » Services » OpenPGP: Sign Selection



PGP/GPG - Cont.

- New Email
  - Ctrl-Click » Services » OpenPGP: Encrypt Selection
  - Select Recipients
  - Send!





PGP/GPG - Cont.

- What about receiving emails?
- Open it up in a text editor!

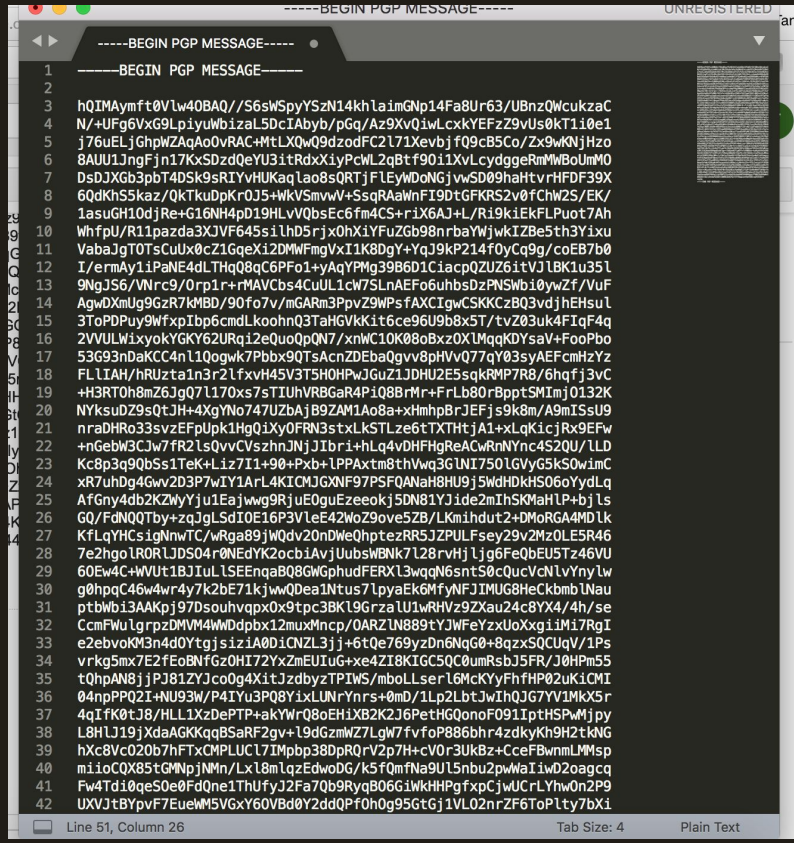
Zhouyu Qian

12:21 PM (23 minutes ago)

to me

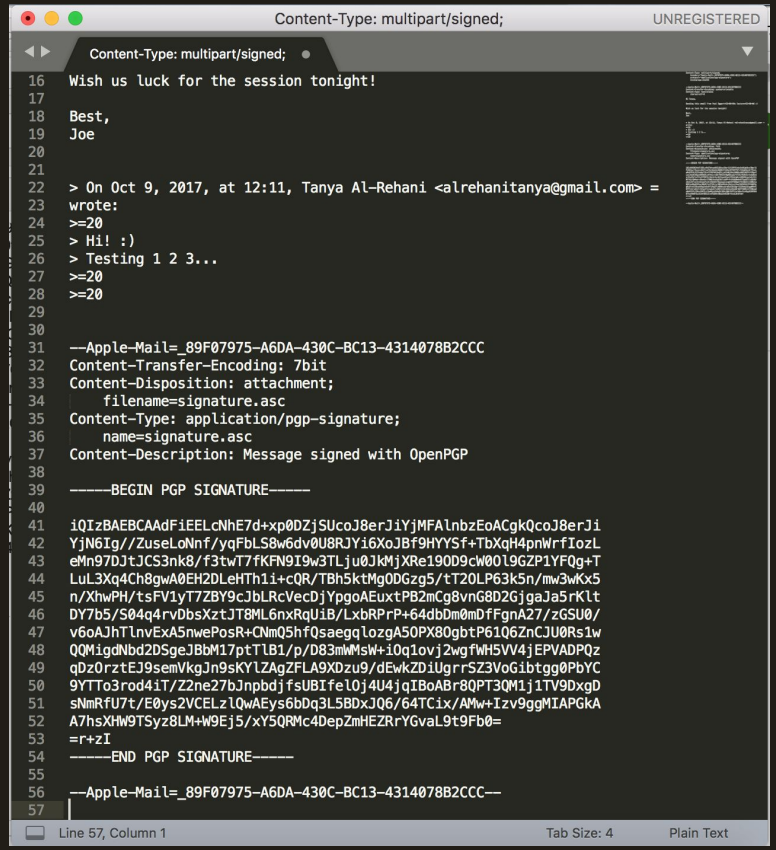
-----BEGIN PGP MESSAGE-----

hQIMAymft0Vlw4OBAQ//S6sWSpyYSzN14khlaimGNp14Fa8Ur63/UBnzQWcukzaC
N/+UFg6VxG9LpiyuWbizaL5DclAbyb/pGq/Az9XvQiwLcxkYEFzZ9vUs0kT1i0e1
j76uELjGhpWZAqAoOvRAC+MtLXQwQ9dzodFC2l71XevbjfQ9cB5Co/Zx9wKNjHzo
8AUU1JngFjn17KxSDzdQeYU3itRdxXiyPcWL2qBtf9Oi1XvLcydggeRmMWBoUmMO
DsDJXGb3pbT4DSk9sRIYvHUKaqlao8sQRTjFlEyWDoNGjvwSD09haHtvrHFDF39X
6QdKhS5kaz/QkTkuDpKrOJ5+WkVSmvwV+SsqRAaWnFI9DtGFKRS2v0fChW2S/EK/
1asuGH1OdjRe+G16NH4pD19HLvVQbsEc6fm4CS+riX6AJ+L/Ri9kiEkFLPuot7Ah
WhfpU/R11pazda3XJVF645silhD5rjxOhXiYFuZGb98nrbaYWjwkIZBe5th3Yixu
VabaJgTOTsCuUx0cZ1GqeXi2DMWFmgVxI1K8DgY+YqJ9kP214fOyCq9g/coEB7b0
I/ermAy1iPaNE4dLTHqQ8qC6PFo1+yAqYPMg39B6D1CiacpQZUZ6itVJlBK1u35l
9NgJS6/VNrc9/Orp1r+rMAVCbs4CuUL1cW7SLnAEFo6uhbsDzPNSWbi0ywZf/VuF
AgwDXmUg9GzR7kMBD/9Ofo7v/mGARm3PpvZ9WPsfAXCIgwCSKKCzBQ3vdjhEHsul
3ToPDPuy9WfxpIbp6cmdLkoohnQ3TaHGVkKit6ce96U9b8x5T/tvZ03uk4FIqF4q
2VVULWixyokYGKY62URqi2eQuoQpQN7/xnWC1OK08oBxzOXlMqqKDYsaV+FooPbo
53G93nDaKCC4nl1Qogwk7Pbbx9QTsAcnZDEbaQgvv8pHVvQ77qY03syAEFcmHzYz
FLlIAH/hRUzta1n3r2lfxvH45V3T5HOHPwJGuZ1JDHU2E5sqkRMP7R8/6hqfj3vC
+H3RTOh8mZ6JgQ7l17Oxs7sTIUhVRBGaR4PiQ8BrMr+FrLb8OrBpptSMImjO132K
NYksuDZ9sQtJH+4XgYNo747UZbAjB9ZAM1Ao8a+xHmhpBrJEFjs9k8m/A9mISsU9
nraDHRo33svzEFpUpk1HgQiXyOFRN3stxLkSTLze6tTXTHtjA1+xLqKicjRx9EFw
+nGebW3CJw7fR2lsQvvCVszhnJNjJIbri+hLq4vDHFHgReACwRnNYnc4S2QU/lLD
Kc8p3q9QbSs1TeK+Liz7I1+90+Pxb+lPPAxtm8thVwq3GlNI75OlGVyG5kSOwimC
xR7uhDg4Gwv2D3P7wIY1ArL4KICMJGXNF97PSFQANaH8HU9j5WdHDkHSO6oYydLq
AfGny4db2KZWyYju1Eajwwg9RjuEOguEzeeokj5DN81YJide2mIhSKMaHlP+bjls
GQ/FdNQQTby+zqJgLSdIOE16P3VleE42WoZ9ove5ZB/LKmihdut2+DMoRGA4MDlk
KfLqYHCsigNnwTC/wRga89jWQdv2OnDWeQhptezRR5JZPULFsey29v2MzOLE5R46
7e2hgolRORlJDSO4r0NEdYK2ocbiAvjUubsWBNk7l28rvHjljg6FeQbEU5Tz46VU
6OEw4C+WVUt1BJIuLlSEEnqaBQ8GWGphudFERXl3wqqN6sntS0cQucVcNlvYnylw
g0hpqC46w4wr4y7k2bE71kjwwQDea1Ntus7lpyaEk6MfyNFJIMUG8HeCkbmblNau
ptbWbi3AAKpj97Dsouhvqpx0x9tpc3BKl9GrzalU1wRHVz9ZXau24c8YX4/4h/se
CcmFWulgrpzDMVM4WWDdpbx12muxMncp/OARZlN889tYJWFeYzxUoXxgiiMi7RgI
e2ebvoKM3n4dOYtgjsiziA0DiCNZL3jj+6tQe769yzDn6NqG0+8qzxSQCUqV/1Ps
vrkg5mx7E2fEoBNfGzOHI72YxZmEUIuG+xe4ZI8KIGC5QC0umRsbJ5FR/J0HPm55
tQhpAN8jjPJ81ZYJcoOg4XitJzdbyzTPIWS/mboLLserl6McKYyFhfHP02uKiCMI
04npPPQ2I+NU93W/P4IYu3PQ8YixLUNrYnrs+0mD/1Lp2LbtJwIhQJG7YV1MkX5r
4qIfK0tJ8/HLL1XzDePTP+akYWrQ8oEHiXB2K2J6PetHGQonoFO91IptHSPwMjpy
L8HlJ19jXdaAGKKqqBSaRF2gv+l9dGzmWZ7LgW7fvfoP886bhr4zdkyKh9H2tkNG
hXc8VcO2Ob7hFTxCMPLUCl7IMpbp38DpRQrV2p7H+cVOr3UkBz+CceFBwnmLMMsp
miioCQX85tGMNpjNMn/Lxl8mlqzEdwoDG/k5fQmfNa9Ul5nbu2pwWaIiwD2oagcq
Fw4Tdi0qeSOe0FdQne1ThUfyJ2Fa7Qb9RyqBO6GiWkHHPgfxpCjwUCrLYhwOn2P9
UXVJtBYpvF7EueWM5VGxY6OVBd0Y2ddQPfOhQg95GtGj1VLO2nrZF6ToPlty7bXi

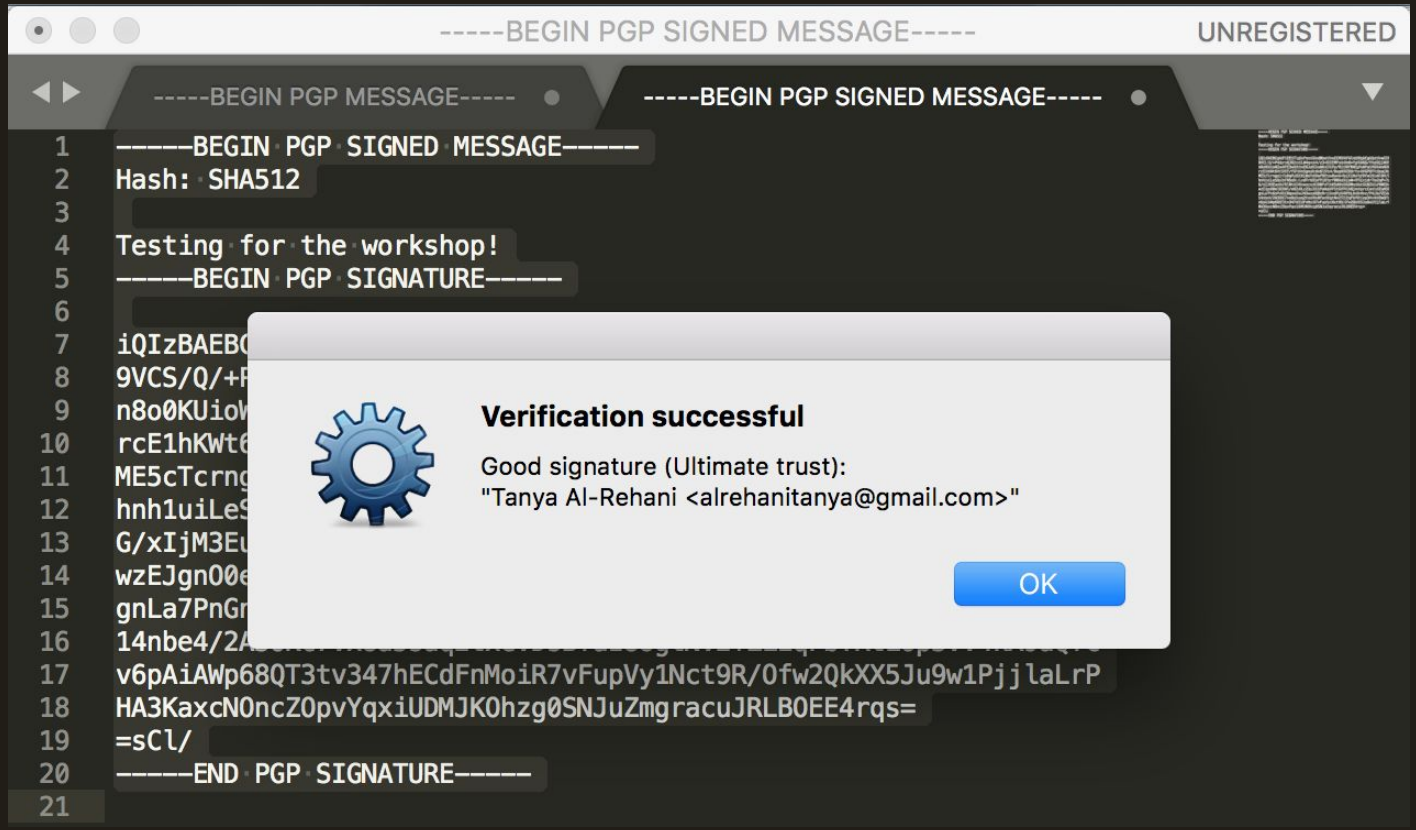


PGP/GPG - Cont.

- Use the shortcuts we defined earlier!
- ^⌥⌘-
  - Decrypt
- ^⌥⌘]
  - Verify Signature

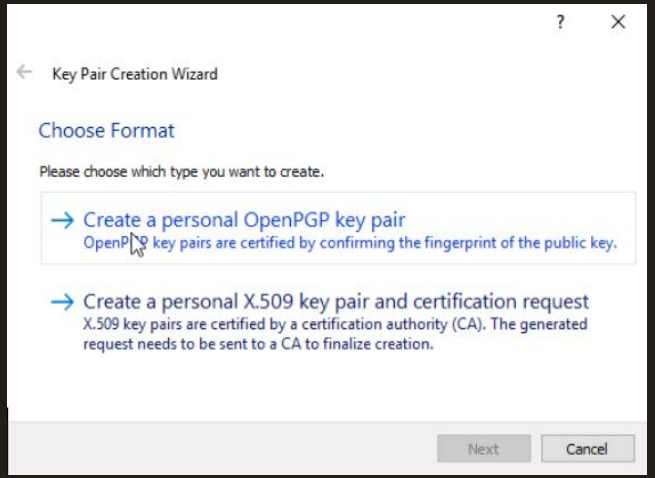


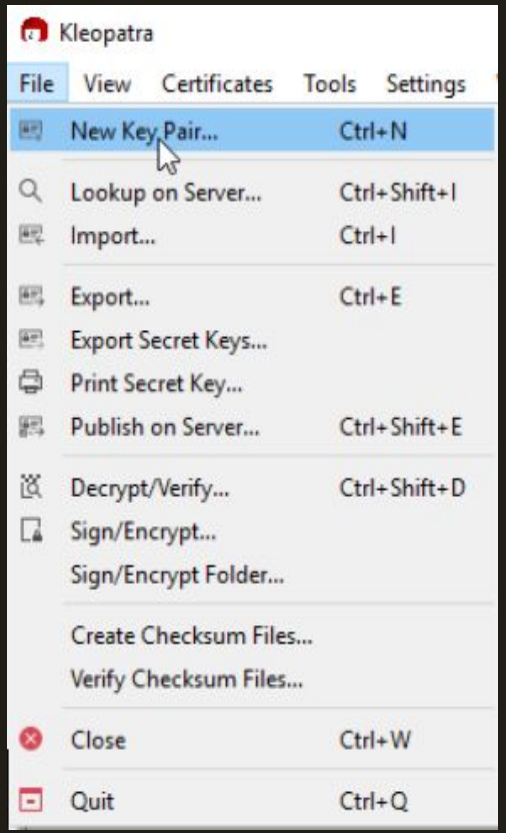
PGP/GPG - Cont.


-----BEGIN PGP SIGNED MESSAGE-----
UNREGISTERED
-----BEGIN PGP MESSAGE-----
-----BEGIN PGP SIGNED MESSAGE-----
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512
Testing for the workshop!
-----BEGIN PGP SIGNATURE-----
v6pAiAWp68QT3tv347hECdFnMoiR7vFupVy1Nct9R/Ofw2QkXX5Ju9w1PjjlaLrP
HA3KaxcNOncZOpvYqxiUDMJKOhzg0SNJuZmgracuJRLBOEE4rqs=
=sCl/
-----END PGP SIGNATURE-----
Verification successful
Good signature (Ultimate trust):
"Tanya Al-Rehani <alrehanitanya@gmail.com>"
OK

GPG for Windows - create

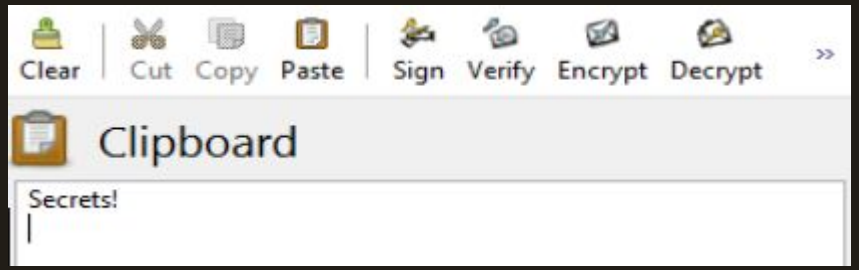
- Install https://www.gpg4win.org
- Make new key pair in Kleopatra

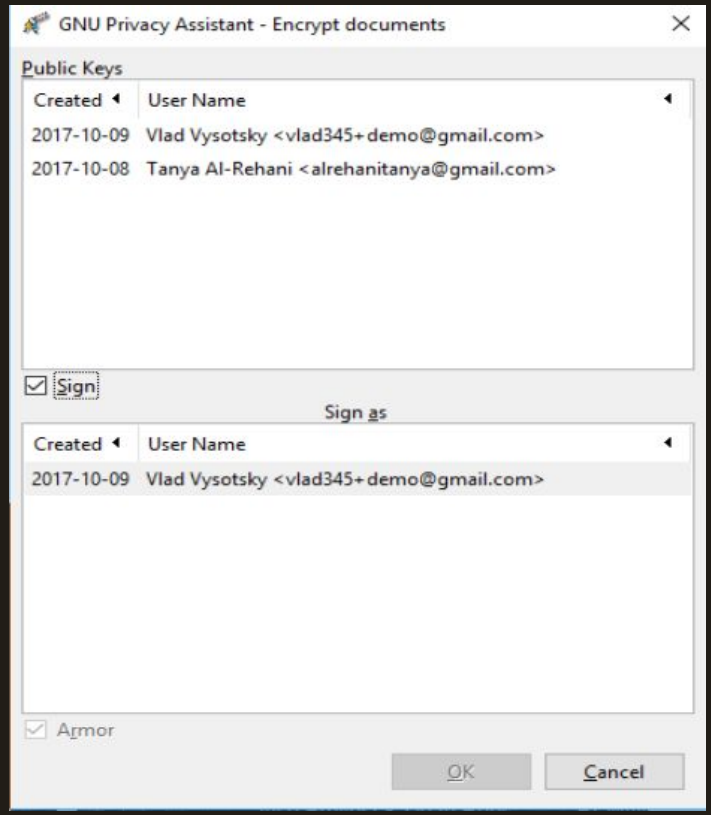




GPG for Windows - send

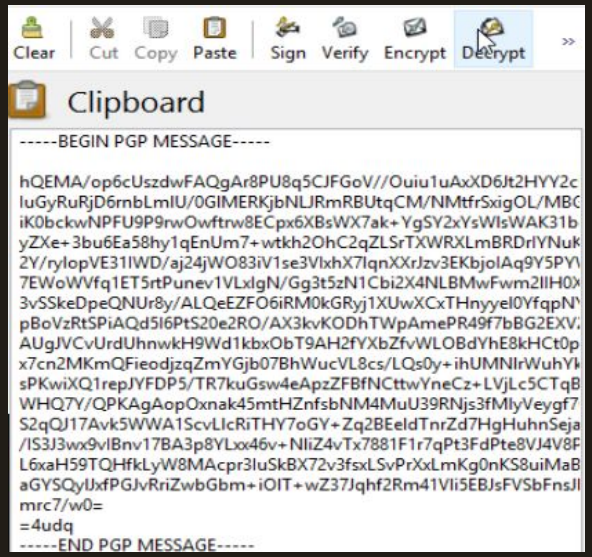
- Switch to GNU Privacy Assistant
- Compose message and encrypt (optionally sign)

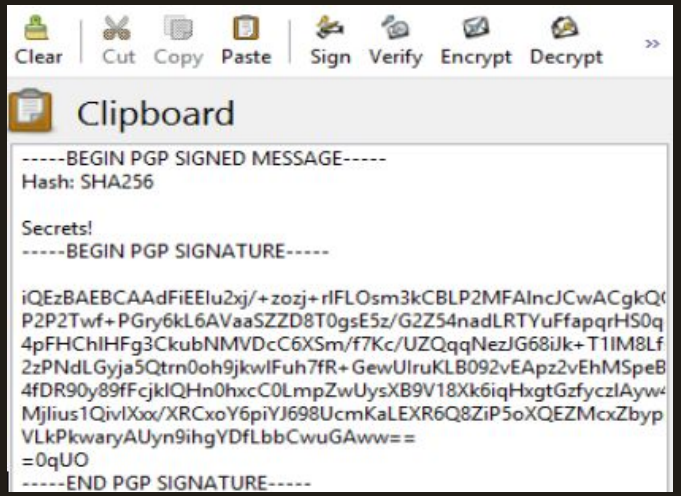


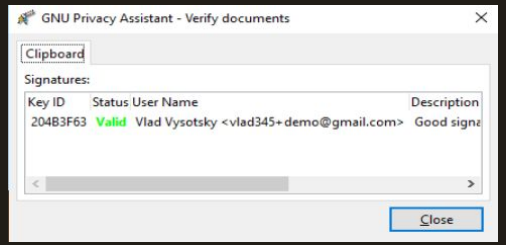


GPG for Windows - receive

- The same process, but in reverse

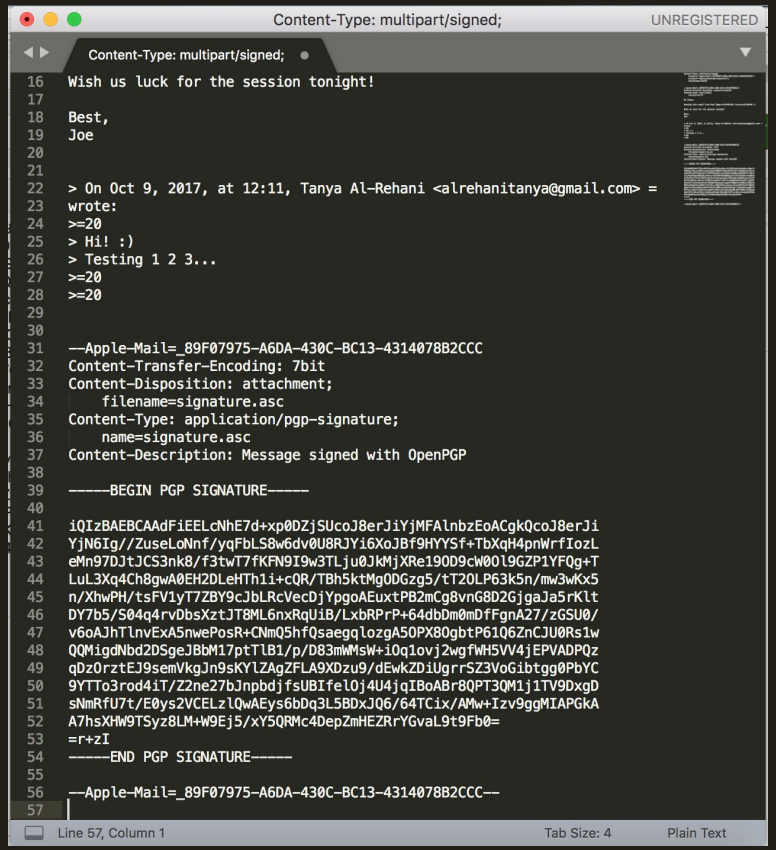






PGP/GPG - Cont.

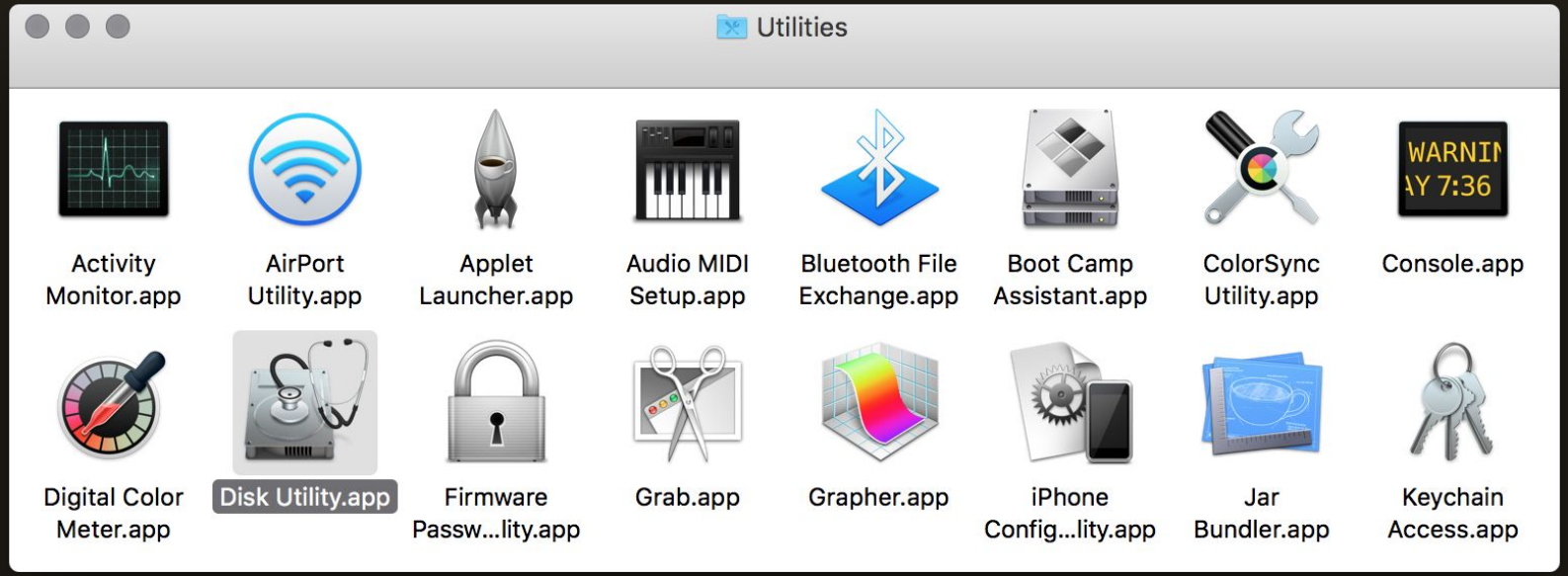
- Options:
  - Nothing - no security
  - Sign, don't encrypt
    - Not confidential
  - Sign AND encrypt
- Tools
  - Mail plugins
  - Command Line https://www.gnupg.org/documentation/manpage.html
  - https://www.phildev.net/pgp/pgp_clear_vs_mime.html
- Defect: http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.html



Practical file encryption

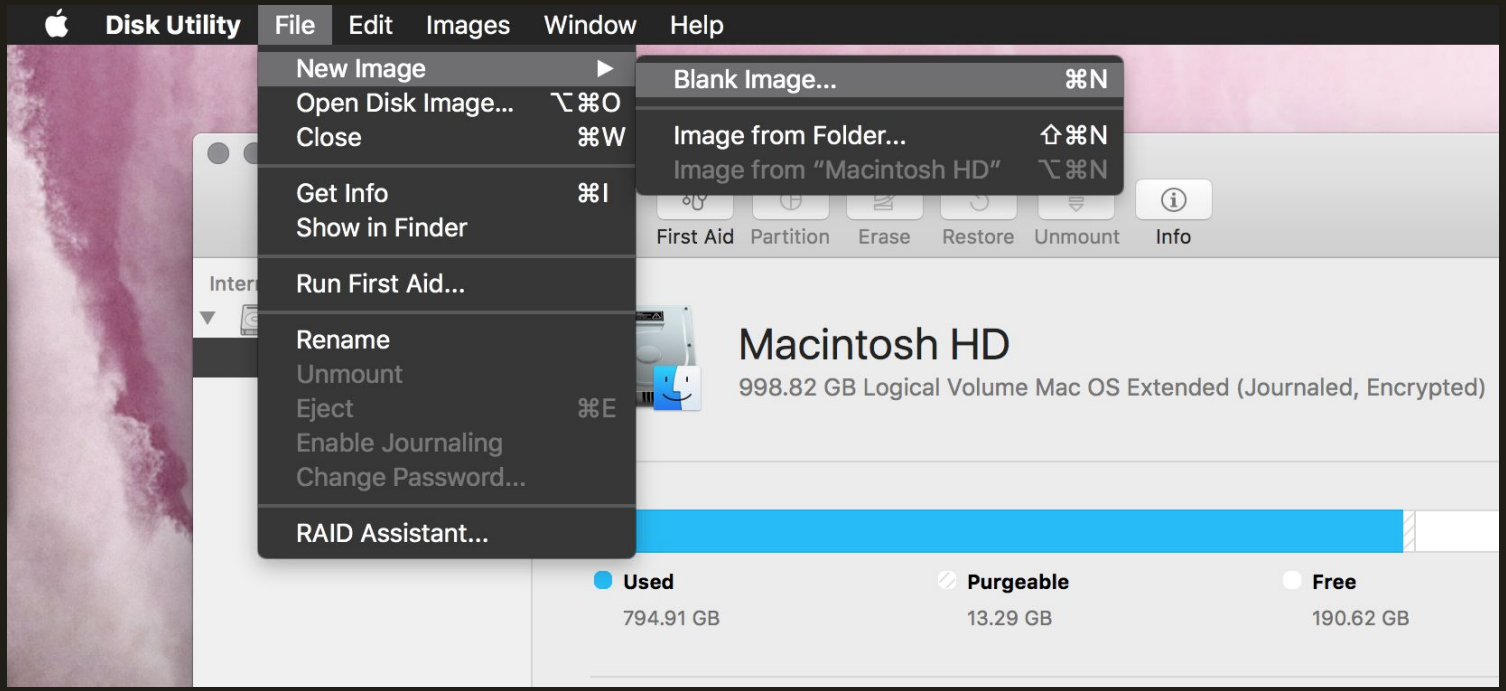
- Did you find using PGP/GPG troublesome?
- If you:
  - do not care about open source/free software (i.e. you trust your software vendor);
  - do not wish to install extra software;
  - value simplicity, user-friendliness, and good platform integration;
  - do not wish your encrypted files to be cross-platform; and
  - do not mind a couple megabytes of overhead of a filesystem;
- Then there is an easier way to encrypt your files!
- Beware that it works differently on macOS, on Linux and on Windows. :(

Practical file encryption (Mac)



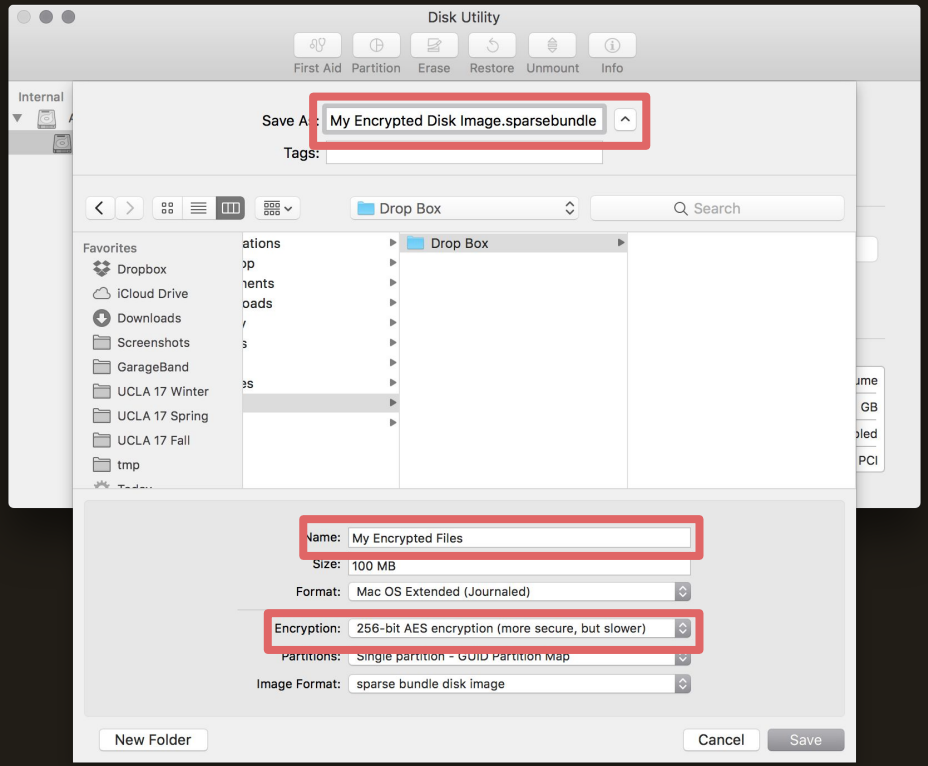
Step One: Find the Disk Utility app inside the /Applications/Utilities folder on your Mac.

Practical file encryption (Mac)



Step Two: Choose “File » New Image » Blank Image...”.

Practical file encryption (Mac)

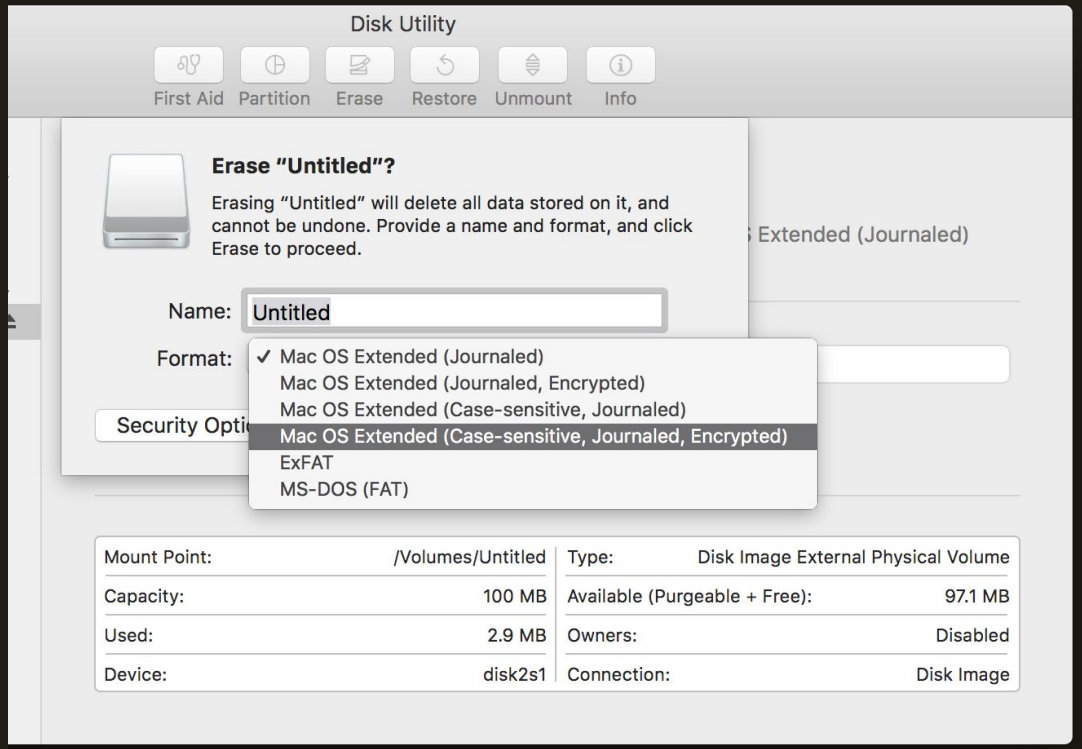


Step Three: Enable encryption!

Practical file encryption (Mac)

Step Four: Et voilà!

Practical file encryption (Mac): An Alternative



Here is a different way of enabling file encryption. Instead of creating an encrypted disk image, you can encrypt a whole disk using Core Storage! This is usually more suitable for whole partitions and whole disks (although you can use it on disk images too).

Practical file encryption (Mac): Terminal Aficionados

```
$ hdiutil create -size 2g -type SPARSEBUNDLE -fs JHFS+ -volname 'My Encrypted Volume' -attach -encryption AES-256 -stdinpass ./Image.sparsebundle
```

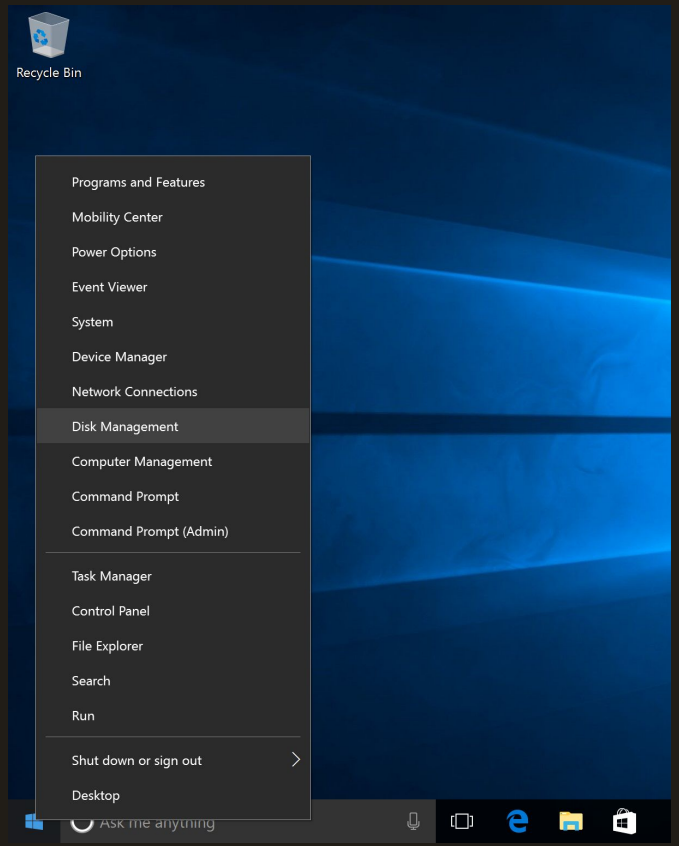
```
$ diskutil cs create 'My Volume Group' disk1s1

$ diskutil cs createVolume 11111111-2222-3333-4444-555555555555 jhfs+ 'My Encrypted Volume' '100%' -stdinpassphrase
```

Practical file encryption (Mac)

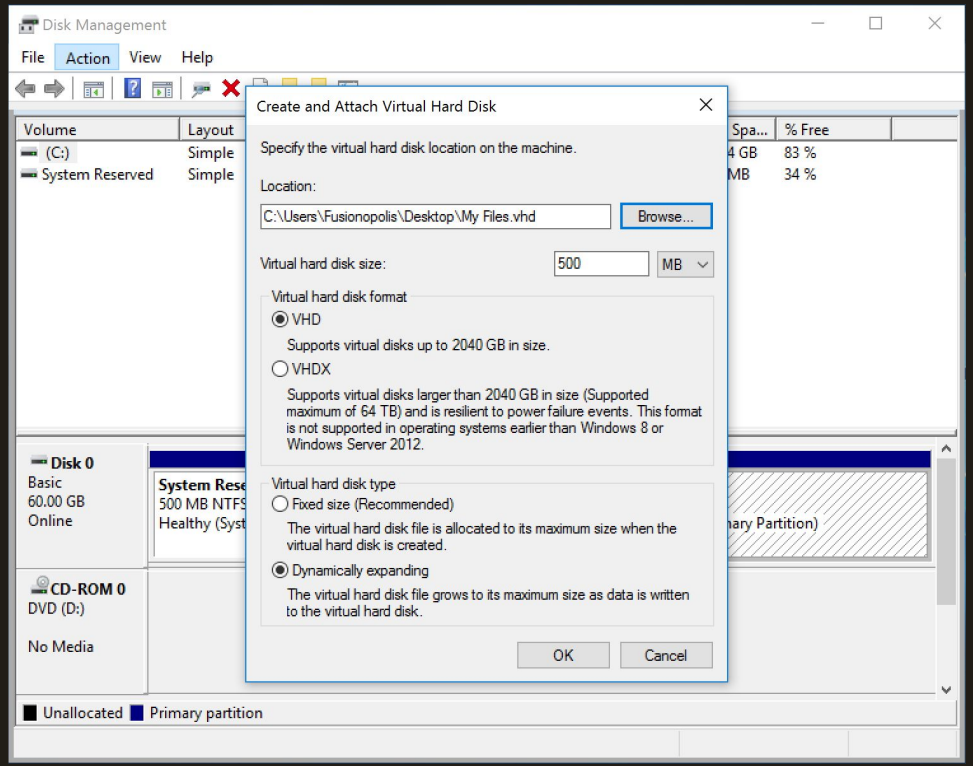
In both cases, remember to ⌘E the drive when you're done!

Practical file encryption (Windows)



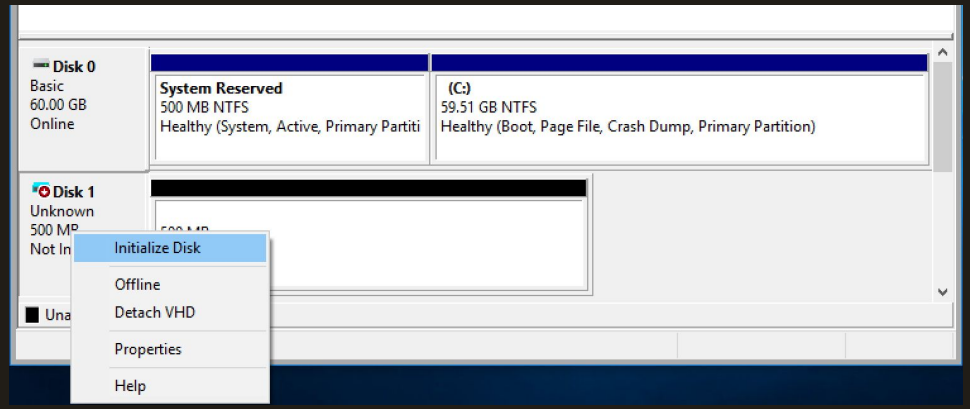
Step One: Open Disk Management tool (a plugin for the Microsoft Management Console) by right-clicking the Start button, or open `diskmgmt.msc`

Practical file encryption (Windows)



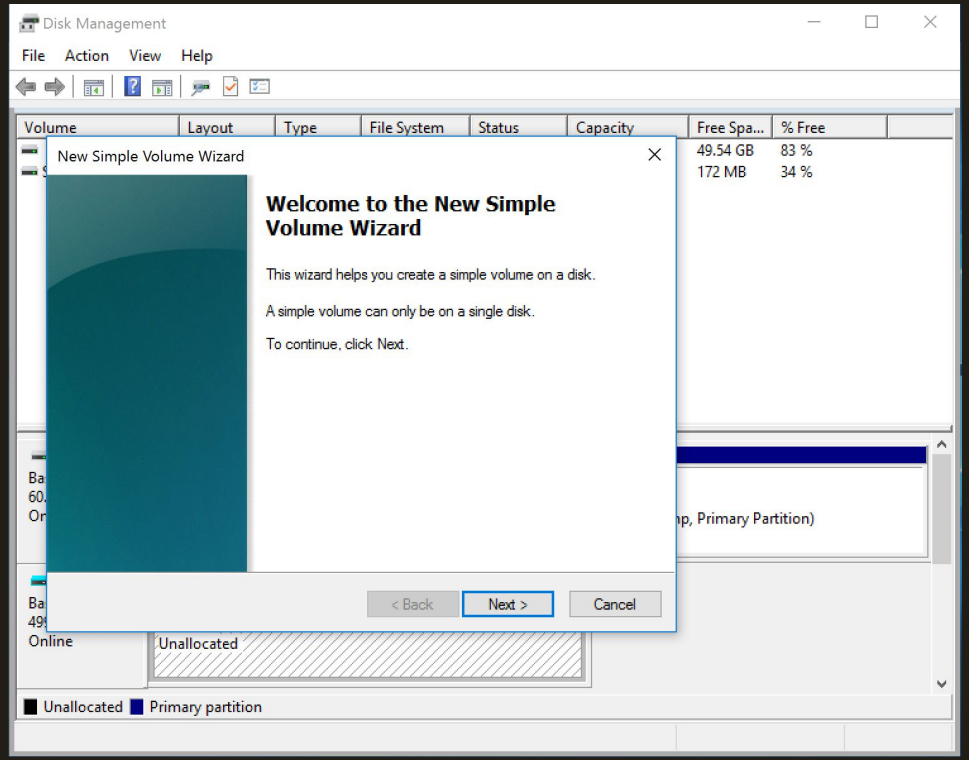
Step Two: Choose “Action » Create VHD” to create a virtual hard disk

Practical file encryption (Windows)



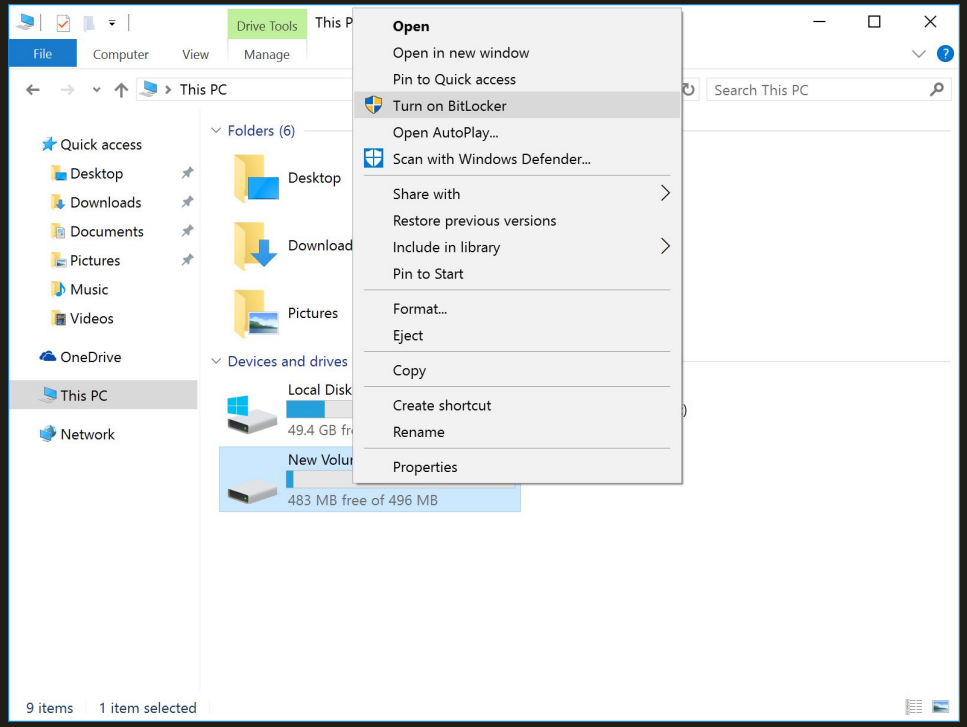
Step Three: Right click on the new disk and choose to “initialize disk”

Practical file encryption (Windows)



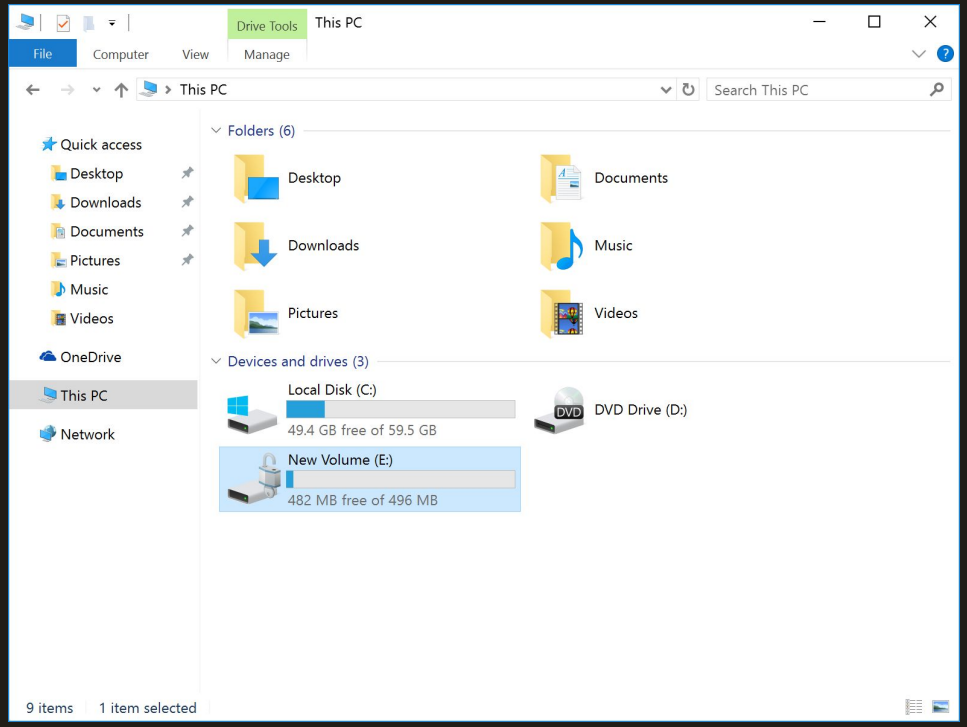
Step Four: Right click on the unallocated space and choose “New Simple Volume...”, then click “Next” four times followed by “Finish”

Practical file encryption (Windows)



Step Five: Go to “This PC” and right click on the new volume just created. Choose “Turn on BitLocker”

Practical file encryption (Windows)



Step Six: After clicking “Next” a few more times (saving recovery keys, etc), your encrypted drive is created! Et voilà! Look at the lock icon next to your new drive!

Practical file encryption (Windows)

Remember to right click and “Eject” the drive when you’re done!

Credits to Frank Chen

https://kfrankc.me/cs88s/