



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!)



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!)



Why

Why

Why

Why

Why

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



National Cyber Security
Awareness Month

Keeping UCLA Safe
It's Our Shared
Responsibility

Visit www.security.ucla.edu



@UCLA_ITSecurity

UCLA IT Services

Russian hacking warrants
sanctions, cybersecurity CEO
says

Anita Balakrishnan | @MsABalakrishnan
Tuesday, 27 Dec 2016 | 3:30 PM ET



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

Giuliani as Trump's cybersecurity
adviser is an unfunny joke

There's a new sheriff in hacker town, and nobody takes him seriously.

Violet Blue, @violetblue
01.20.17 In Security

141
Comments

3046
Shares





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 



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

Why

Why

Why

Why

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



2. The Hackable Cardiac Devices from St. Jude

Cyber-Safe

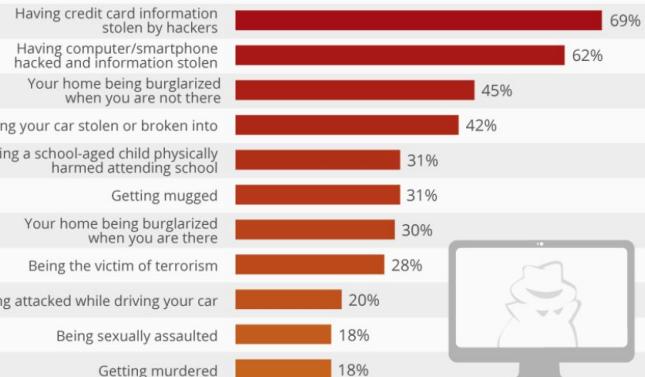
Cybercrime costs the average U.S. firm \$15 million a year

by James Griffiths @CNNTech

October 8, 2015 3:28 AM ET

Hacking Has Become Every American's Worst Nightmare

% of Americans who frequently or occasionally worry about the following



@StatistaCharts Source: Gallup



Why

Why

Why

Why

Why

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

Why

Why

Why

Why

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)

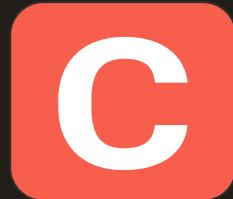




Agenda

- 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

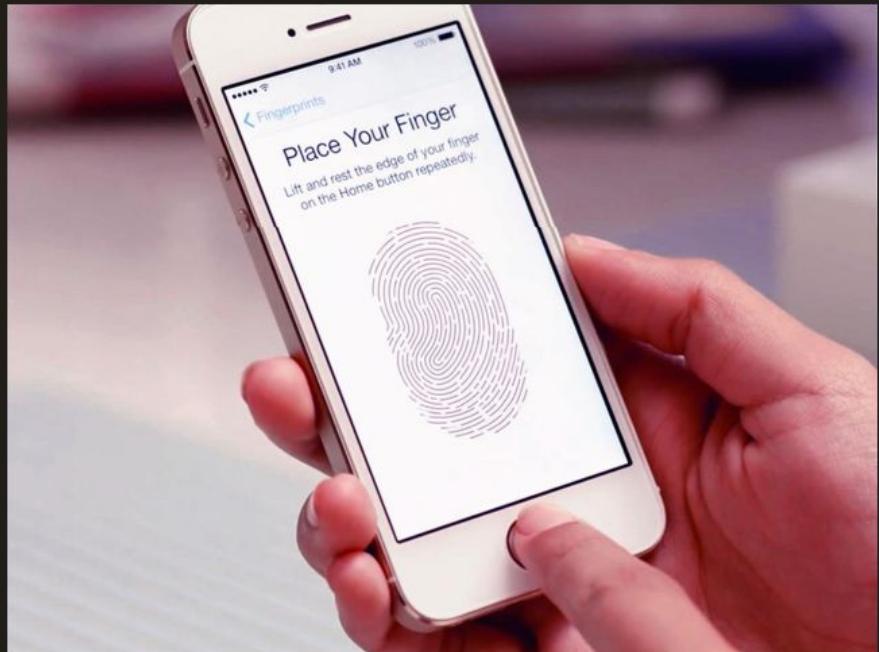
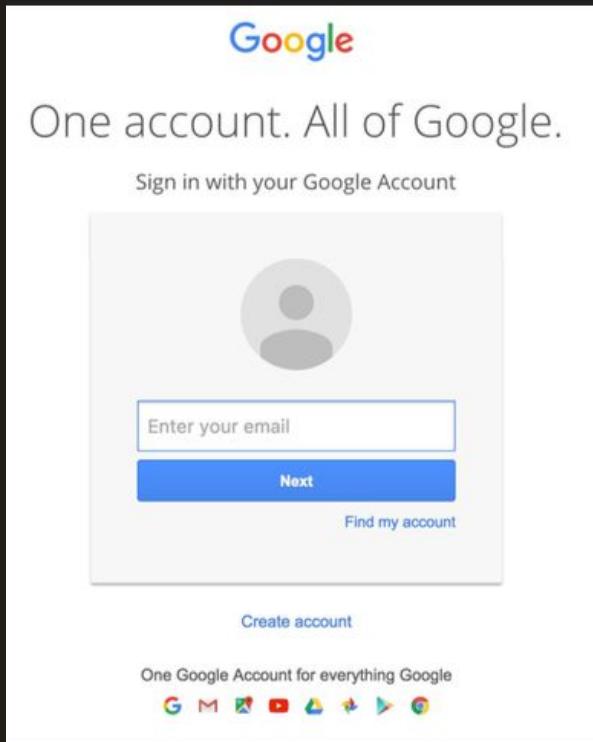


Confidentiality



Confidentiality:

Ability to hide information from those people unauthorized to view it





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.





Availability

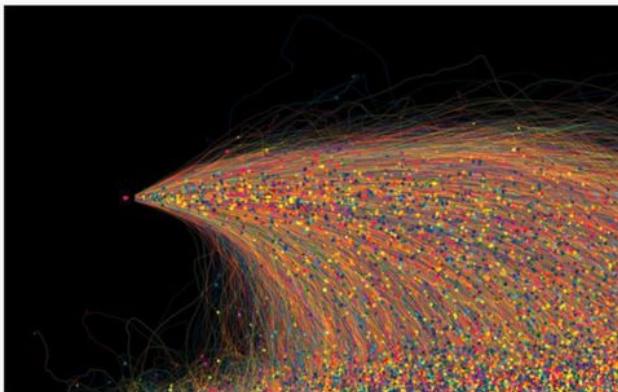


Availability:

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

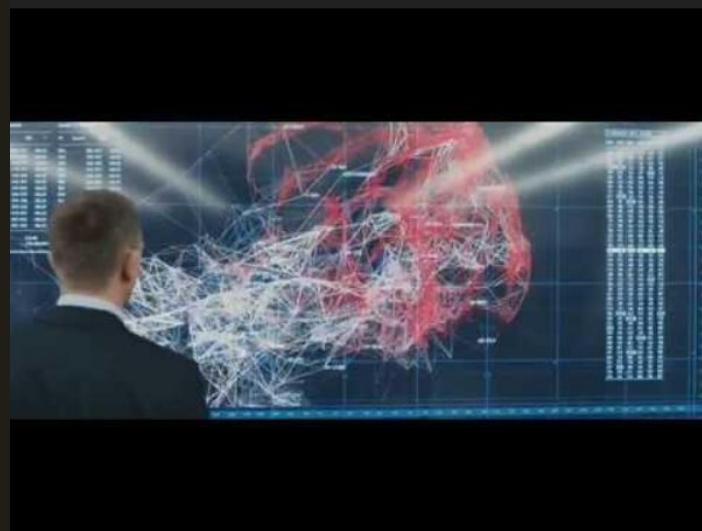


<https://www.youtube.com/watch?v=bb0EHcA-71I&feature=youtu.be>

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=q6qG-6Co_v4



What was good about that?

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

MR. ROBOT VS SKYFALL

007™

- 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: ⌘-Shift-D
 - Encrypt: ⌘-Shift-E
 - Sign: ⌘-Shift-S
 - Verify: ⌘-Shift-V



GPGMail

is an open source plugin for Apple Mail. Encrypt, decrypt, sign and verify mails using OpenPGP with a few simple clicks.



GPG Keychain

is an open source application for macOS. It allows you to manage your OpenPGP keys. Create and modify your keys and import the keys of your friends from a key server.



GPG Services

is a plugin that brings GPG power to almost any application. It allows you to encrypt/decrypt, sign/verify and import keys from text selections, files, folders and much more.



MacGPG

is the underlying power engine of GPG Suite. If you're familiar with the command line use the raw power of it. Based on GnuPG.



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 Test

qzy@qzy.io

PGP Test

;) Testing 1 2 3...

-----BEGIN PGP SIGNATURE-----

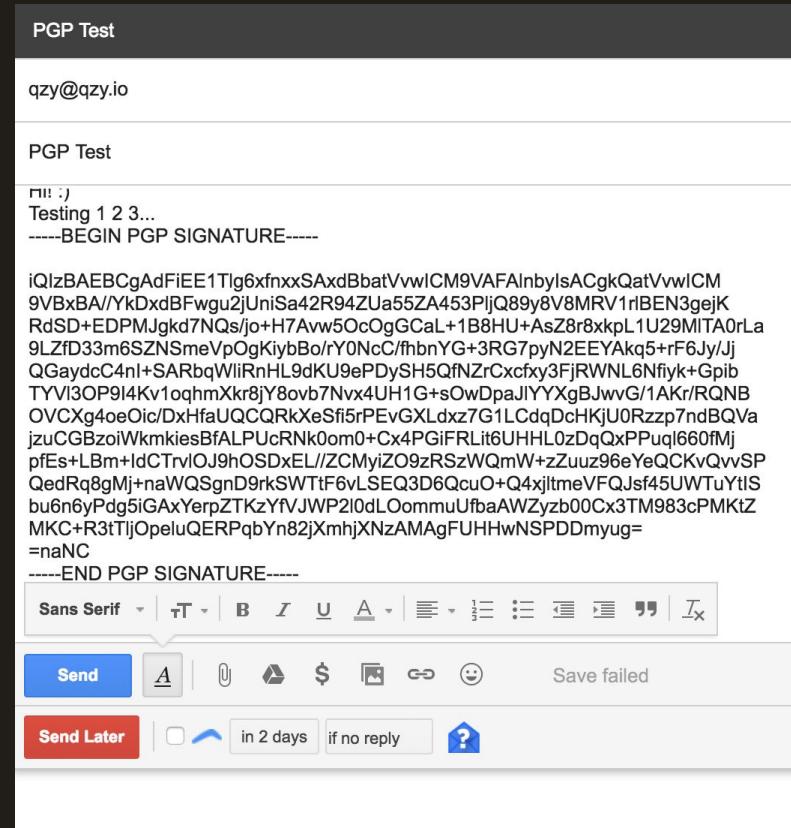
iQIzBAEBCgAdFiEE1Tlg6xfnxSAXdBbatVvwICM9VAFAlnbyIsACgkQatVvwICM9VBxBA/YkDxdBFwgu2jUniSa42R94ZUa55ZA453PljQ89y8V8MRV1rIBEN3gejKRdSD+EDPMJgkd7NQs/jo+H7Avw5OcOgGCaL+1B8HU+AsZ8r8xkpL1U29MITA0rLa9LzfD33m6SZNSmeVpOgKiybBo/rY0NcC/fhbnYG+3RG7pyN2EEYAkq5+F6Jy/JjQGaydcC4nI+SARbqWlRnHL9dKU9ePDySH5QfNzCxcfxy3FjRWNL6Nfiyk+GpibTYVi3OP9i4Kv1oqhmXkr8jY8ovb7Nvx4UH1G+sOwDpaJYYXgBJwvG/1AkR/RQNB0VCXg4oeOic/DxHfaUQCQRkXeSi5rPEvGXLDxz7G1LCdqDcHQjU0Rzzp7ndBQVajzuCGBzoiWkmkiesBfALPUcRNk0om0+Cx4PGiFRLit6UHHLOzDqQxPPuql660fMjpfEs+LBm+IdCTrvlOJ9hOSDxEI/ZCMyiZO9zRSzWQmW+zZuuZ96eYeQCKvQvvSPQedRq8gmJ+naWQSgnD9rkSWTf6vLSEQ3D6QcuO+Q4xjlmeVFQjsf45UWTuYIISbu6n6yPdg5iGAxYerpZKzYfVJWP2l0dLoommuUfbawWZyzb00Cx3TM983cPMKtZMKC+R3TljOpeluQERPqbYn82jXmhjXNzAMAgFUHhwNSPDDmyug=

=naNC

-----END PGP SIGNATURE-----

Sans Serif Save failed

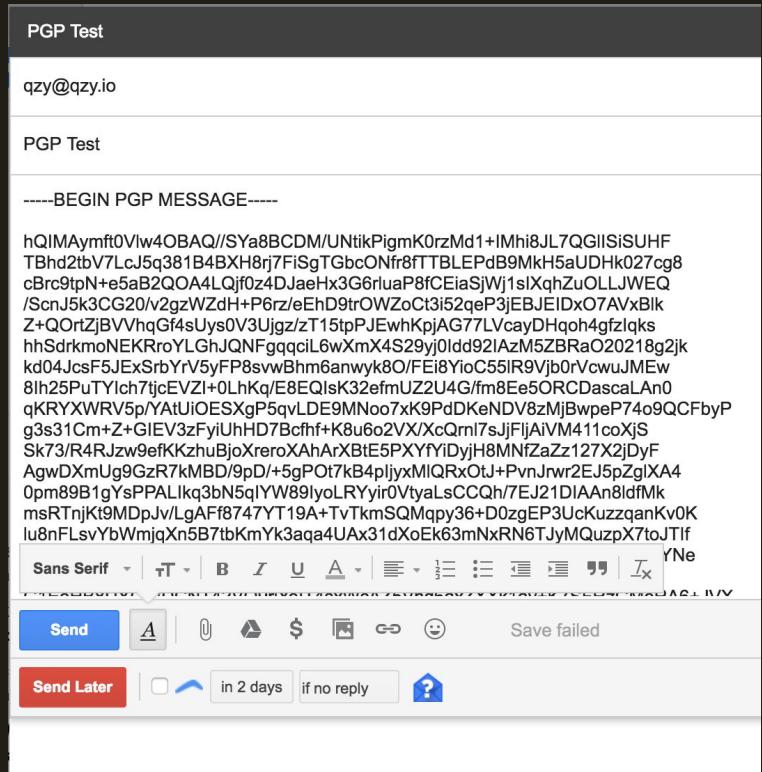
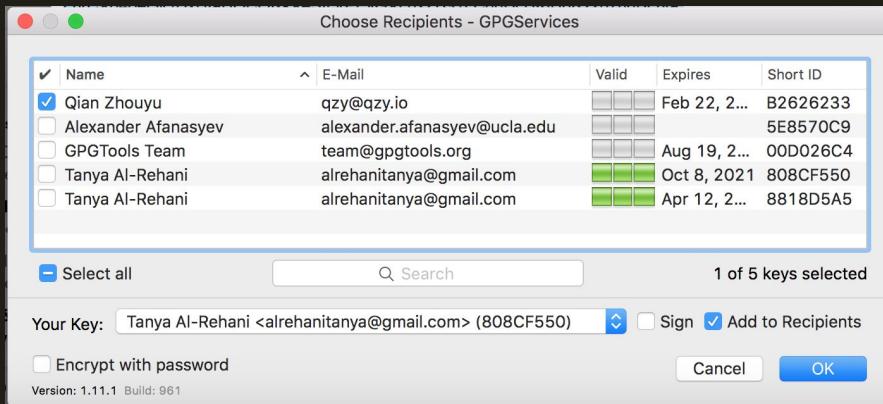
in 2 days if no reply





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-----

```
hQIMAyamft0Vlw4OBaQ/S6sWSpYSzN14khlaImGnp14Fa8Ur63/UBnzQWcukzaC
N/+UFg6VxG9LpiyuWbzal5DcIAbyp/gQ/Az9XvQiwlCxkYEfZ9vUs0kT1i0e1
j76uELjGhpwZAqAo0vRAC+MTLXQwQ9dZodFC2l71Kevbjf09cb5Co/Zx9wKnJhzo
8AUU1ngFjn17KsDzDq0YeU3itRdxXiyoPwL2qBtF90i1vLcydggeRmWB0uImMO
DsJXGb3pbT4DSk9sR1YYHUKaqaloa8s0RTjFLeYwDoNGjvwSd09haHtrhFDF39X
6Qdkh5KaZ/qTKtdpGr0J5+wKvSmwvV+SsqRAawnf1o9dtGFKRs2v0fchW2S/EK/
1asuGH10dJre+G16NH4pD19HLv0bseCcfn4CS+riXgAjl-L/R19k1EkfLPuot7Ah
WhfpU/R11pazda3XJVF645si1hD5rjx0hXiYFuZgb98nrbawjwklZBe5th3ixu
VabaJgTOTScuUx0cZ1GqeX12DMWFmgVx1K1B0DgY+YqJ9kP214f0yCq9g/coEB7b0
I/ermAYi1PaNE4dLTHq08qC6PF01+yqYPMg39B601ciacpZU261tVjBk1u35l
9NgJS6/Vnrc9/0rp1+r+RMV/Cbs4cuLwC7SwLAEfo6uhbsdzPNsWbliywZf/Vuf
AgwDXmUg9GzR7kMBD/90f07v/mGArM3PpvZ9WPsfAXCIgwCSKKCzBQ3vdjhEhsuL
3ToPDPuy9Wfpb6cmdkloohnQ3TaHGvKkIt6ce96U9bd8xT/tvZ03uk4FqF4q
2VVULWixoykYGK62URq12eo0u0Pn7/xnWC10K08ob8xz0XIMqqDysaV-FooPbo
53G93nDaKCC4n1QogwktPbbx9QtAcnZDebaQgvv8pHvv077qY03syAEFcmlHzYz
FLIAH/hRUzta1n3r2lfxv145V3T5HOHpwJGUz1JDHU2E5sqkRMP7R8/6hfqj3vC
+H3RT0hbmZ6Jq0717Oxs7sTUHvRBGaq4PjQ8BrMr+FrLb80RpptSMImj0132K
NYksuDZ6jsQtlJh+4XgYN0747UzbA1B92AM1A08a+xhlmhpBrJEfj9k8m/A9mIsstU9
nraDRo33svzEfpupk1Hq0g1N0R3ntsLkStLze6tTXTHtjA1+xLqKicjRx9EfW
+nGeb3CJw7fR2lsQvvCvzshnJNj1Bir+hLq4vDHFhgrReAcwRnNyNc4s2Qu/LD
Kc8p3q9Bs1TeK+liz71+90+PPAxmt8hwv3GIN750iGVyG5kS0winC
xR7uhDg4Gw2D3P7w1Y1Ar4LKMjGXNF97PSFQANaH8HUi9j5wDhDkHS06oYydlq
AfGny4Dp92KMyJu1Eajwgw9Rjue0guEzeekoj5DN81Yjde2mhsKMaHIP+bjls
GQ/FdNQQTby+zqJgLsDlOE16P3leE42zw09ve52BLkmhdut2+Dm0RGA4MDlk
KfLqYHCSigNwTC/wRga9jWQd20nDWeQptezRR5JZPULfsey29/MzOLE5R46
7e2hgoIROLRJDSO4/0NEdyK2ocblAvJubswBNK7128rvHljljg6FeQbU5Tz46VU
6OEw4C+WWU1Bj2lrxvEneq9BQ8HpwGphudFERxi3wqqNsnst50cQuCvNvNyrlw
g0hpcC46w4w4ry7k2bE71kjw0Dea1ntus7lpyaEk6myFnFIJMUGhEcKbmbnNau
ptbWbi3AAKpj97Dsouhvxqpx0x9tpc3BK19GrzalU1wRHvZ9Zxau24c8YX4/4h/se
CcmFWulgrpzDMV4MwDdpbx12maxMncp/OARZIn889tYJWFeYzxUoXggiMi7RqI
e2ebvoKm3n4dYttgjzis1A0D1cnZL3j+6t0e769yzDnGnQG0+8qzqSOQuqV/1Ps
vrkg5Mx7F2FeBnFg20H72YxZmEU1uG-xe4Z8K1Gc5QC0umRsbJ5FR/J0HPm55
tQhpAn3svzEfUpk1Hq0g1N0R3ntsLkStLze6tTXTHtjA1+xLqKicjRx9EfW
60Ew4C+WWU1Bj2lrxvEneq9BQ8HpwGphudFERxi3wqqNsnst50cQuCvNvNyrlw
g0hpcC46w4w4ry7k2bE71kjw0Dea1ntus7lpyaEk6myFnFIJMUGhEcKbmbnNau
ptbWbi3AAKpj97Dsouhvxqpx0x9tpc3BK19GrzalU1wRHvZ9Zxau24c8YX4/4h/se
Afgny4Dp92KMyJu1Eajwgw9Rjue0guEzeekoj5DN81Yjde2mhsKMaHIP+bjls
L8H1Lj19jzAgaDKgwaSarF2yj16DgZmwZL7Lw7fvfop886bh4r2dkyKh9H2tkNG
hXcCv02067hFTxCMPLUCL7IMpb3DpdBqrZp7H+cV0r3UkZb+CceFbwmlLMsp
mioi0pq0eSe0fd0ne1ThUfyJ2Fa70Bw9ryqB06GiwkhHPgfpCwJUcrLhywOn2P9
Fw4Tdi0qeSe0fd0ne1ThUfyJ2Fa70Bw9ryqB06GiwkhHPgfpCwJUcrLhywOn2P9
UXVJtBypfTfEuemW5VGxY60Vb0Y2ddQF0h095GtGj1VL02nZF6ToPlty/bxi
```

-----BEGIN PGP MESSAGE----- UNREGISTERED anya

```
1 -----BEGIN PGP MESSAGE----- 
2 
3 hQIMAyamft0Vlw4OBaQ/S6sWSpYSzN14khlaImGnp14Fa8Ur63/UBnzQWcukzaC
4 N/+UFg6VxG9LpiyuWbzal5DcIAbyp/gQ/Az9XvQiwlCxkYEfZ9vUs0kT1i0e1
5 j76uELjGhpwZAqAo0vRAC+MTLXQwQ9dZodFC2l71Kevbjf09cb5Co/Zx9wKnJhzo
6 8AUU1ngFjn17KsDzDq0YeU3itRdxXiyoPwL2qBtF90i1vLcydggeRmWB0uImMO
7 DsJXGb3pbT4DSk9sR1YYHUKaqaloa8s0RTjFLeYwDoNGjvwSd09haHtrhFDF39X
8 6Qdkh5KaZ/qTKtdpGr0J5+wKvSmwvV+SsqRAawnf1o9dtGFKRs2v0fchW2S/EK/
9 1asuGH10dJre+G16NH4pD19HLv0bseCcfn4CS+riXgAjl-L/R19k1EkfLPuot7Ah
10 WhfpU/R11pazda3XJVF645si1hD5rjx0hXiYFuZgb98nrbawjwklZBe5th3ixu
11 VabaJgTOTScuUx0cZ1GqeX12DMWFmgVx1K1B0DgY+YqJ9kP214f0yCq9g/coEB7b0
12 I/ermAYi1PaNE4dLTHq08qC6PF01+yqYPMg39B601ciacpZU261tVjBk1u35l
13 9NgJS6/Vnrc9/0rp1+r+RMV/Cbs4cuLwC7SwLAEfo6uhbsdzPNsWbliywZf/Vuf
14 AgwDXmUg9GzR7kMBD/90f07v/mGArM3PpvZ9WPsfAXCIgwCSKKCzBQ3vdjhEhsuL
15 3ToPDPuy9Wfpb6cmdkloohnQ3TaHGvKkIt6ce96U9bd8xT/tvZ03uk4FqF4q
16 2VVULWixoykYGK62URq12eo0u0Pn7/xnWC10K08ob8xz0XIMqqDysaV-FooPbo
17 53G93nDaKCC4n1QogwktPbbx9QtAcnZDebaQgvv8pHvv077qY03syAEFcmlHzYz
18 FLIAH/hRUzta1n3r2lfxv145V3T5HOHpwJGUz1JDHU2E5sqkRMP7R8/6hfqj3vC
19 +H3RT0hbmZ6Jq0717Oxs7sTUHvRBGaq4PjQ8BrMr+FrLb80RpptSMImj0132K
20 NYksuDZ6jsQtlJh+4XgYN0747UzbA1B92AM1A08a+xhlmhpBrJEfj9k8m/A9mIsstU9
21 nraDRo33svzEfpupk1Hq0g1N0R3ntsLkStLze6tTXTHtjA1+xLqKicjRx9EfW
22 +nGeb3CJw7fR2lsQvvCvzshnJNj1Bir+hLq4vDHFhgrReAcwRnNyNc4s2Qu/LD
23 Kc8p3q9Bs1TeK+liz71+90+PPAxmt8hwv3GIN750iGVyG5kS0winC
24 xR7uhDg4Gw2D3P7w1Y1Ar4LKMjGXNF97PSFQANaH8HUi9j5wDhDkHS06oYydlq
25 AfGny4Dp92KMyJu1Eajwgw9Rjue0guEzeekoj5DN81Yjde2mhsKMaHIP+bjls
26 G0/QPf0h09wzqJLSDi0E5Pv3Lee42w0Z9ove5ZB/L/kmihdu7+Dm0RGA4MDlk
27 KfLqYHCSigNwTC/wRga9jWQd20nDWeQptezRR5JZPULfsey29/MzOLE5R46
28 7e2hgolR0LJDS04/rNEdyK2ocblAvjUubswnk7128rvHljljg6FeQbU5Tz46VU
29 60Ew4C+WWU1Bj2lrxvEneq9BQ8HpwGphudFERxi3wqqNsnst50cQuCvNvNyrlw
30 g0hpcC46w4w4ry7k2bE71kjw0Dea1ntus7lpyaEk6myFnFIJMUGhEcKbmbnNau
31 ptbWbi3AAKpj97Dsouhvxqpx0x9tpc3BK19GrzalU1wRHvZ9Zxau24c8YX4/4h/se
32 CcmFWulgrpzDMV4MwDdpbx12maxMncp/OARZIn889tYJWFeYzxUoXggiMi7RqI
33 e2ebvoKm3n4dYttgjzis1A0D1cnZL3j+6t0e769yzDnGnQG0+8qzqSOQuqV/1Ps
34 vrkg5Mx7F2FeBnFg20H72YxZmEU1uG-xe4Z8K1Gc5QC0umRsbJ5FR/J0HPm55
35 tQhpAn3svzEfUpk1Hq0g1N0R3ntsLkStLze6tTXTHtjA1+xLqKicjRx9EfW
36 04npPPQ21+iNu3W/P41YU3P8yixLUnRyrs+0mD/lpl2bJw1hJG7Y1MKx5r
37 4qfK0tJ8/HLL1XzDePtp+2aywR08oFh1M26j6tHgQ0noFO91IptHSpMjpy
38 L8H1Lj19jzAgaDKgwaSarF2yj16DgZmwZL7Lw7fvfop886bh4r2dkyKh9H2tkNG
39 hXcCv02067hFTxCMPLUCL7IMpb3DpdBqrZp7H+cV0r3UkZb+CceFbwmlLMsp
40 mioi0pq0eSe0fd0ne1ThUfyJ2Fa70Bw9ryqB06GiwkhHPgfpCwJUcrLhywOn2P9
41 Fw4Tdi0qeSe0fd0ne1ThUfyJ2Fa70Bw9ryqB06GiwkhHPgfpCwJUcrLhywOn2P9
42 UXVJtBypfTfEuemW5VGxY60Vb0Y2ddQF0h095GtGj1VL02nZF6ToPlty/bxi
```

Line 51, Column 26 Tab Size: 4 Plain Text



PGP/GPG - Cont.

- Use the shortcuts we defined earlier!
- ^⌘⌫-

 - Decrypt

- ^⌘⌦

 - Verify Signature

```
Content-Type: multipart/signed; boundary=Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC
Content-Type: multipart/signed;
Wish us luck for the session tonight!
Best,
Joe
> On Oct 9, 2017, at 12:11, Tanya Al-Rehani <alrehanitanya@gmail.com> =
wrote:
>=20
> Hi! :)
> Testing 1 2 3...
>=20
>=20
--Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
filename=signature.asc
Content-Type: application/pgp-signature;
name=signature.asc
Content-Description: Message signed with OpenPGP
-----BEGIN PGP SIGNATURE-----
iQIZBAEBCAAAdFiEELnNhe7d+xp0DZjSUcoJ8erJiYjMFAlnbzEoACqkQcoJ8erJi
YjN61g//ZuseLoNf/yqFbLSw6dvU8RJYi6XoJBf9HYY5f+TbXqH4pnWrIozL
eMr97DjtJCS3nk8/f3twT7TKFN919w3TLju0uJMjXRe190d9cw0019GZp1YFQq+T
LuL3Xq4Ch8gwA0EH2DLeHTh11+c0R/TBh5ktMg0DGzg5/tT20LP63k5n/mw3wKx5
n/XhwPH/tsFV1yTZY9cJbLRVecDjYpgoAEuxtPB2mCg8vnG802GjgaJa5rKlt
D7Yb5/S04g4rvDbxZtT8ML6nRxqUiB/LxbRPrp+64dbDm@0mffGgnA27/zGSU0/
v6oAJhTlnvExA5nwePosR+CnnQ5hfQsaeggllozgA50PX80gbtP61062nCJuRs1w
QQMigdNbD2DSgeJBm17ptTlB1/pD83mWMsW+i0q1ovj2wgfWH5V4jEPVADPQz
qD20rzTEJ9semVkgJn9sKyLZAgfzLA9XDzu9/dEwkZDuiLgrRSZ3VoGbttg9PByC
9YTt03rod4iT/Z2n4Eys6bD03LBBDxJ06/64TCix/AMw+Izv9ggMIAPGKA
sNmRFU7t/E0ys2VCELzI0wAEye6bD03LBBDxJ06/64TCix/AMw+Izv9ggMIAPGKA
A7hsXHw9TSyzLmH9E15/xY5QRMc4DepZmHEZRrYGvaL9t9Fb=-
=r+zi
-----END PGP SIGNATURE-----
--Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC--
```

Line 57, Column 1

Tab Size: 4

Plain Text

PGP/GPG - Cont.

-----BEGIN PGP SIGNED MESSAGE----- UNREGISTERED

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

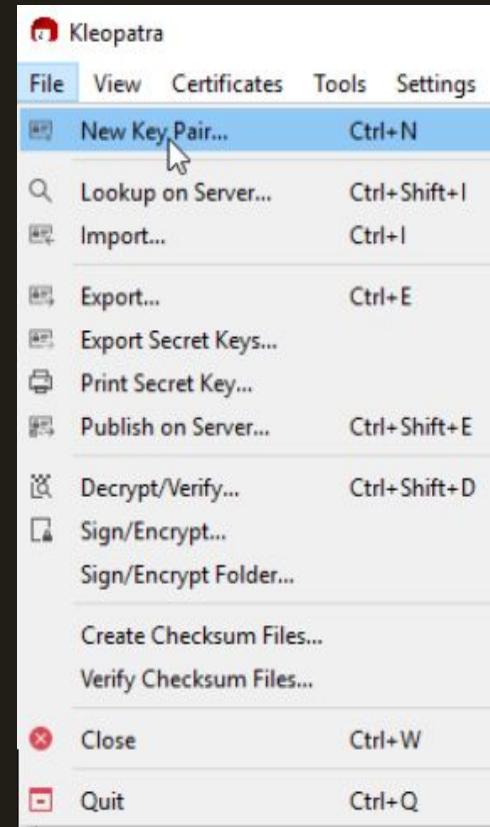
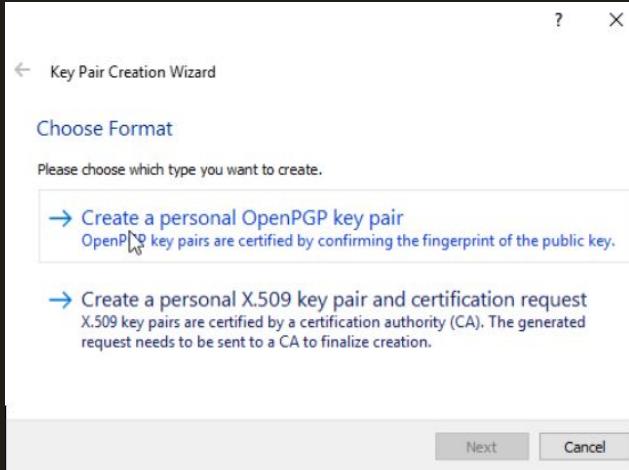
1 -----BEGIN PGP SIGNED MESSAGE-----
2 Hash: SHA512
3
4 Testing for the workshop!
5 -----BEGIN PGP SIGNATURE-----
6
7 iQIzBAEBC
8 9VCS/Q/+R
9 n8o0KUiow
10 rcE1hKwt6
11 ME5cTcrng
12 hnh1uiLeS
13 G/xIJM3Eu
14 wzEJgn00e
15 gnLa7PnGr
16 14nbe4/2A
17 v6pAiAwp68QT3tv347hEcdfNMo iR7vFupVy1Nct9R/0fw2QkXX5Ju9w1PjjlaLrP
18 HA3KaxcN0ncZ0pvYqxiUDMJK0hzg0SNJuZmg racuJRLB0EE4rqs=
19 =sCl/
20 -----END PGP SIGNATURE-----
21

Verification successful
Good signature (Ultimate trust):
"Tanya Al-Rehani <alrehanitanya@gmail.com>"

OK

GPG for Windows - create

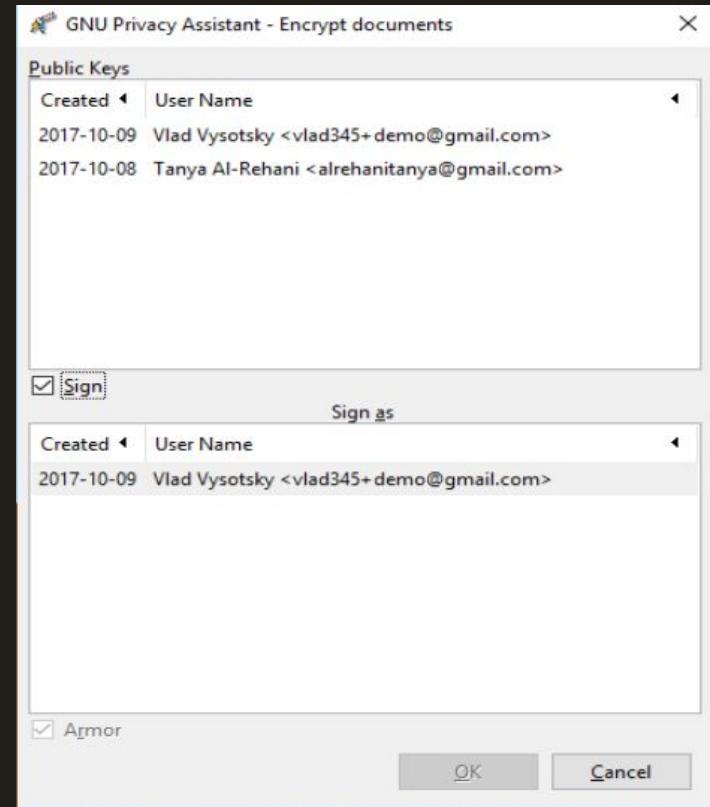
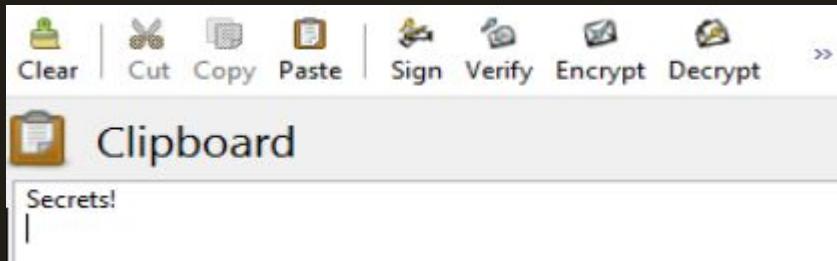
- Install
<https://www.gpg4win.org>
- Make new key pair in Kleopatra





GPG for Windows - send

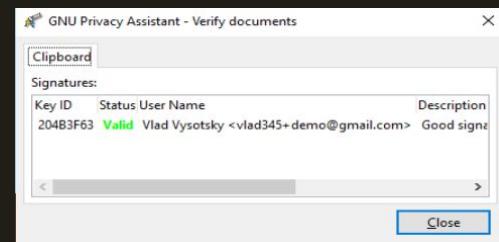
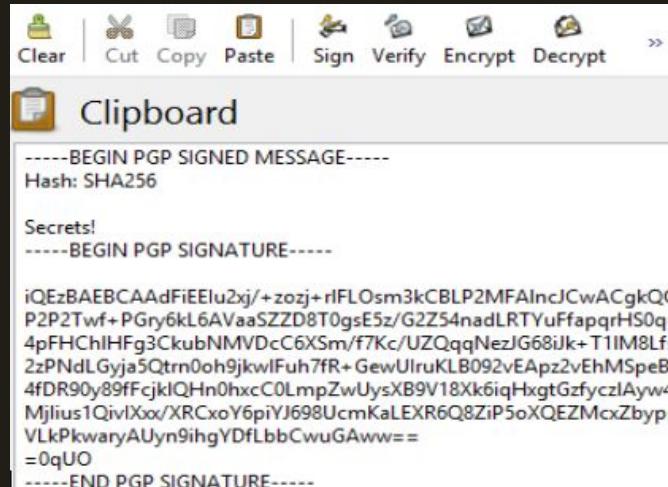
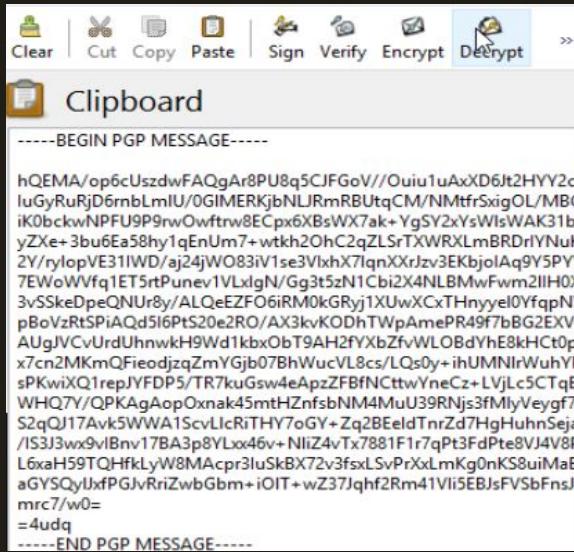
- Switch to GNU Privacy Assistant
- Compose message and encrypt (optionally sign)





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/documents/on/manpage.html>
 - https://www.phildev.net/pgp/pgp_cl ear_vs_mime.html
- Defect:
http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.html

Content-Type: multipart/signed; boundary=Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC
Content-Type: multipart/signed; boundary=Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC
16 Wish us luck for the session tonight!
17
18 Best,
19 Joe
20
21 > On Oct 9, 2017, at 12:11, Tanya Al-Rehani <alrehanitanya@gmail.com> =
22 wrote:
23 =>20
24 > Hi! :)
25 > Testing 1 2 3...
26 =>20
27 =>20
28
29
30
31 --Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC
32 Content-Transfer-Encoding: 7bit
33 Content-Disposition: attachment;
34 filename=signature.asc
35 Content-Type: application/pgp-signature;
36 name=signature.asc
37 Content-Description: Message signed with OpenPGP
38
39 -----BEGIN PGP SIGNATURE-----
40
41 iQIzBAEBCAdfIEELcNhE7d+xp0ZjSUCoJ8erJiYjMFAlnbzEoACqkQcoJ8erJi
42 YjN6Ig//ZuseLoNnf/yqFbLSw6dv0UBRJy16XoJBf9HY5f+tBxqH4pnWrIozL
43 eMr97DjtJCS3nk8/f3tWt7FKFN919w3TLjuu0JKMjXRe190d9cw0019GZP1YFQq+T
44 LuL3Xq4Ch8gw0EH2DLeHTh11+c0R/TBh5ktMg0DGzg5/tT20LP63k5n/mw3wKx5
45 n/XhwPH/t5FV1yTZY9cJblLrcVecDjYpgoAEuxtPBmCg8vnG802Gjga5rKlt
46 DY7b5/S04g4rvDbsXztJ8ML6nxRqxl/B/LxbRRp+64dbDm0mDfFgnA27/zGSU0/
47 v6OAJhTlnvExA5nwePosR+CnnQ5hfQsaegglzogA50PX80gbtP61062ncJU0Rs1w
48 QQMigdNbD2DSeJBbM17ptTLb1/p/D83mMsW+i0q1ovj2wgfWH5VV4jEPVADPQz
49 qD0rzteJ9semVkgJn9sKyLZAgfzLA9XDzu9/dEwkZDuiLgrRSZ3VoGlbttg0PyC
50 9YTTo3rod4iT/ZZne27bjnpbdjfsU81fe1oju44iqIBoABr80PT30M1j1T7V9DxgD
51 sNmHw9T5yz8LM+w9Ej5/xY5QRMc4DepZmHEZRrYGvaL9t9Fb=0
52 =r+zI
53 -----END PGP SIGNATURE-----
54
55 --Apple-Mail=_89F07975-A6DA-430C-BC13-4314078B2CCC--
56
57

Line 57, Column 1 Tab Size: 4 Plain Text

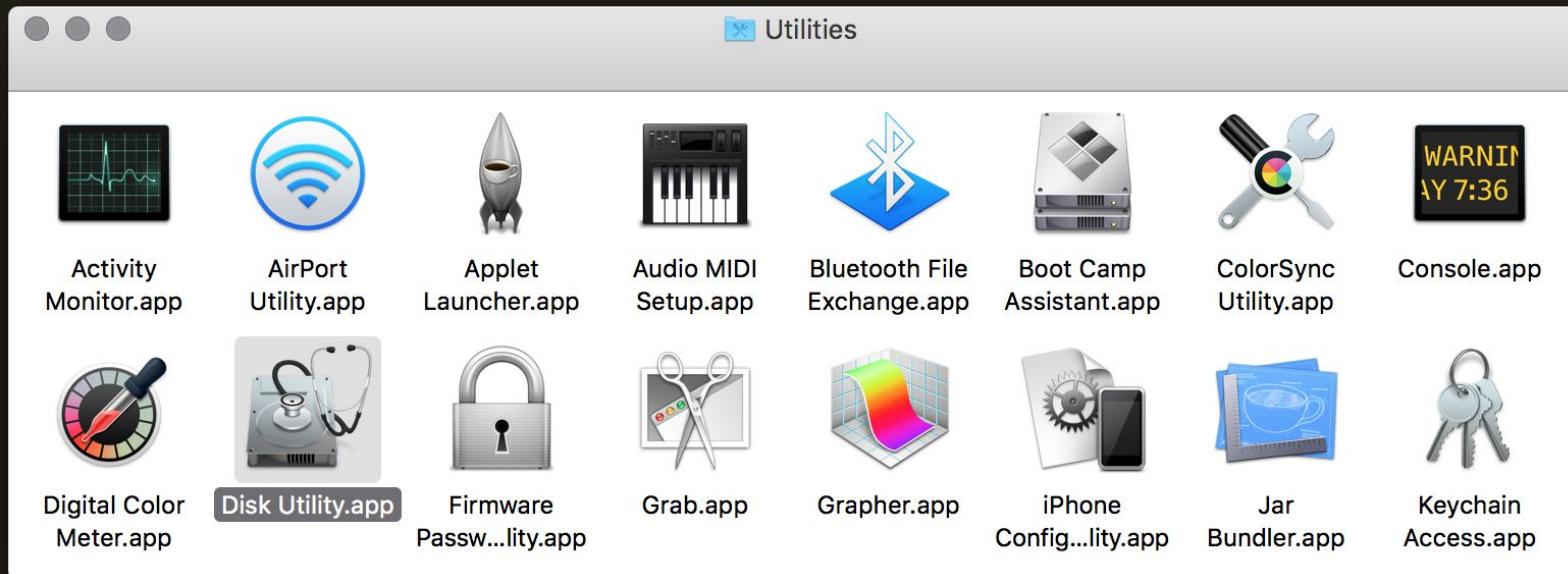


Practical file encryption

- 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. :(

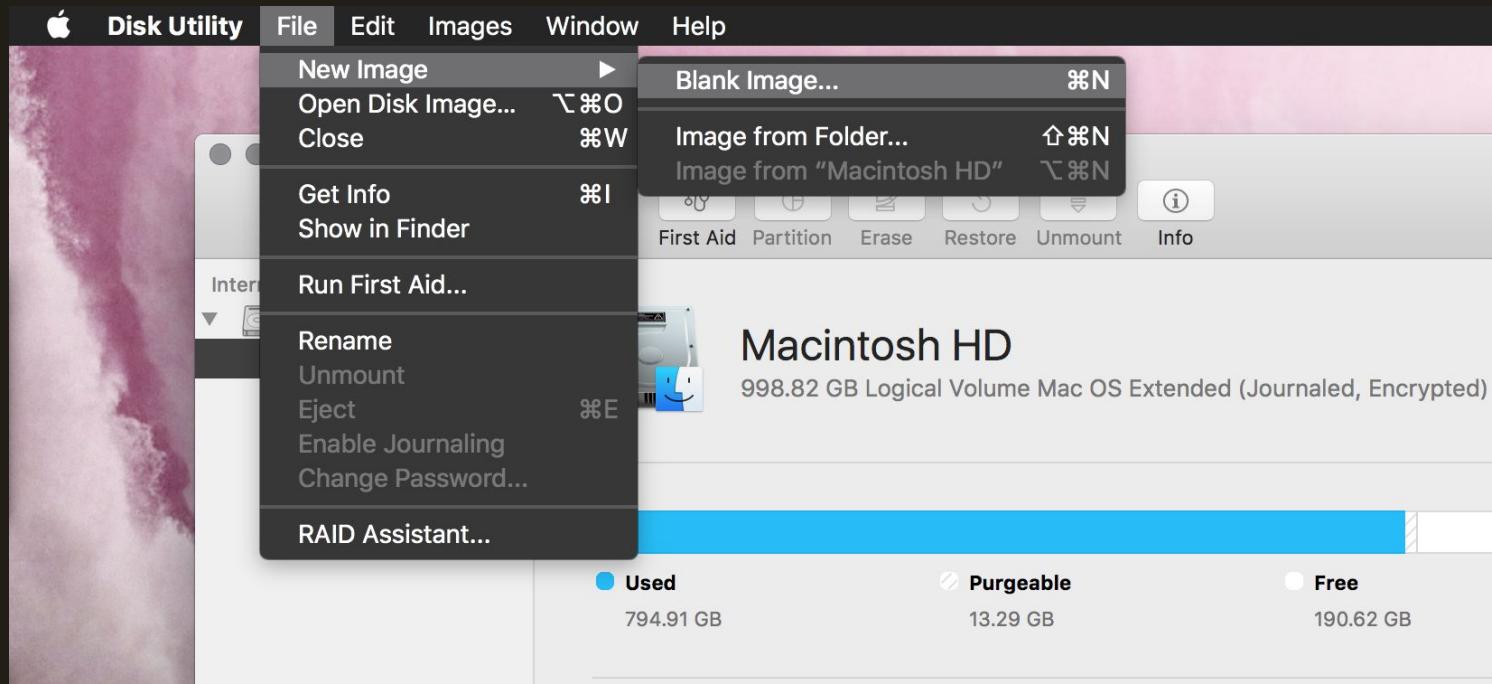


Practical file encryption (Mac)



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

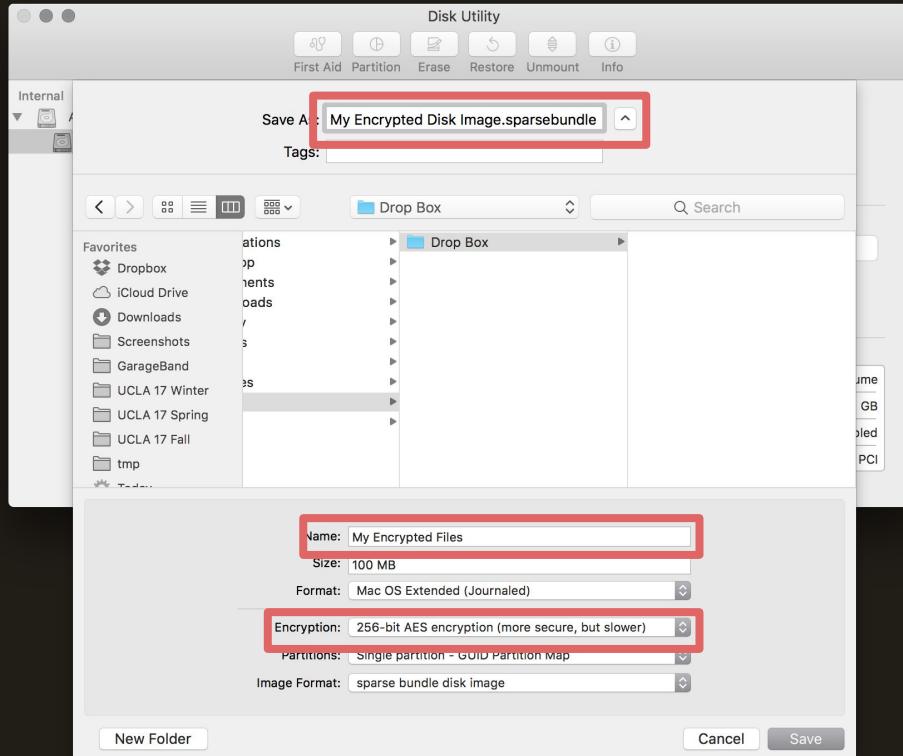
Practical file encryption (Mac)



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



Practical file encryption (Mac)



Step Three: Enable encryption!

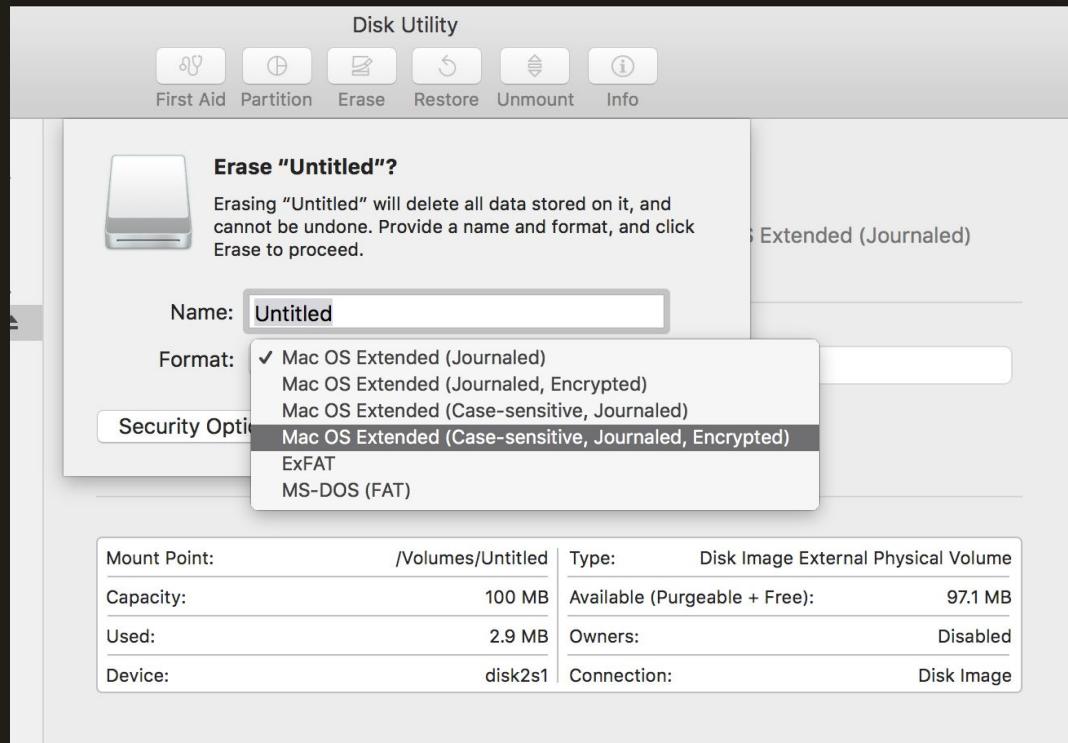


Practical file encryption (Mac)



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
```

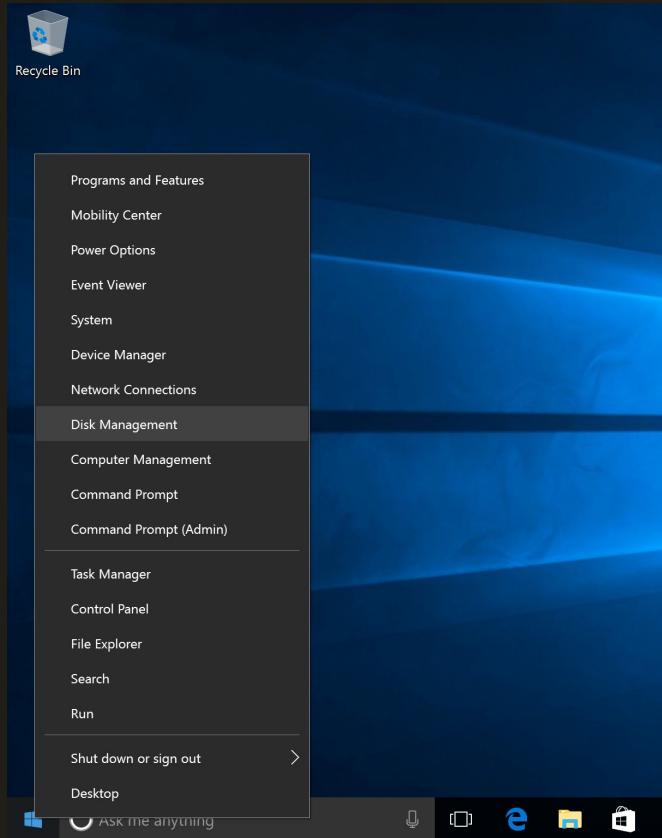
```
$ diskutil cs createVolume 11111111-2222-3333-4444-555555555555 jhfs+ 'My Encrypted Volume' '100%' -stdinpassphrase
```



Practical file encryption (Mac)

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

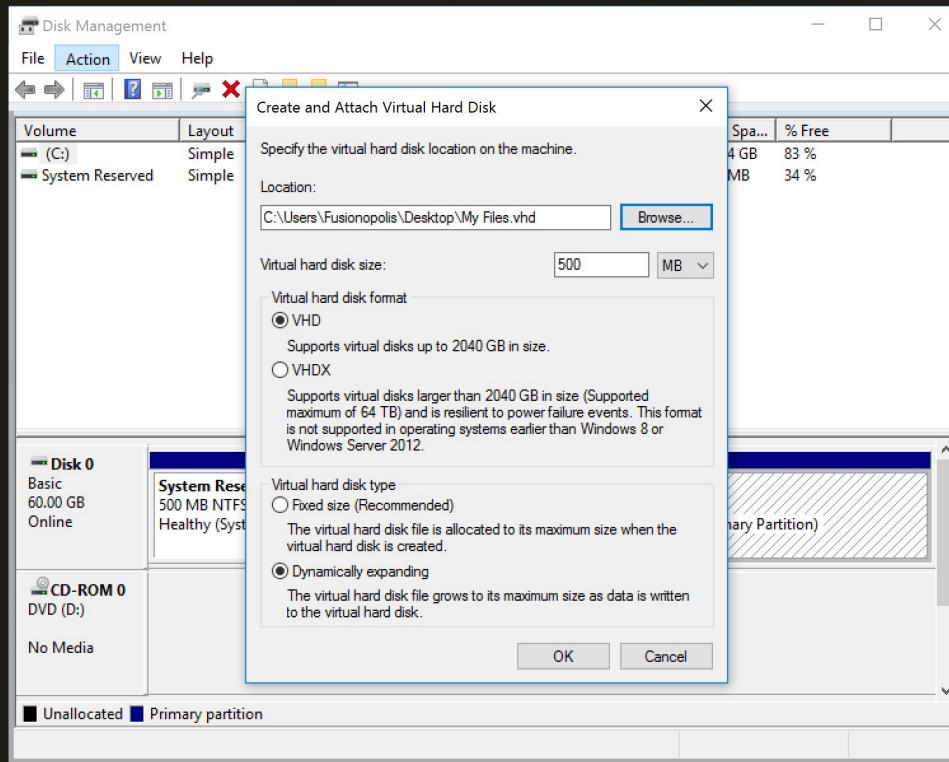
Practical file encryption (Windows)



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

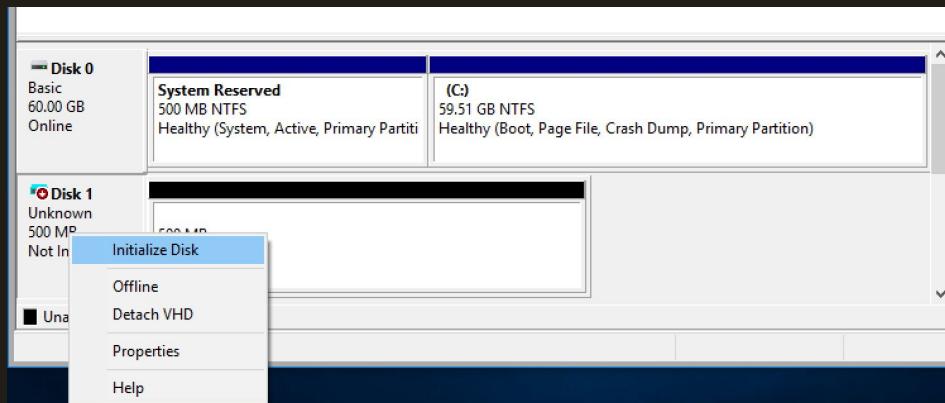


Practical file encryption (Windows)



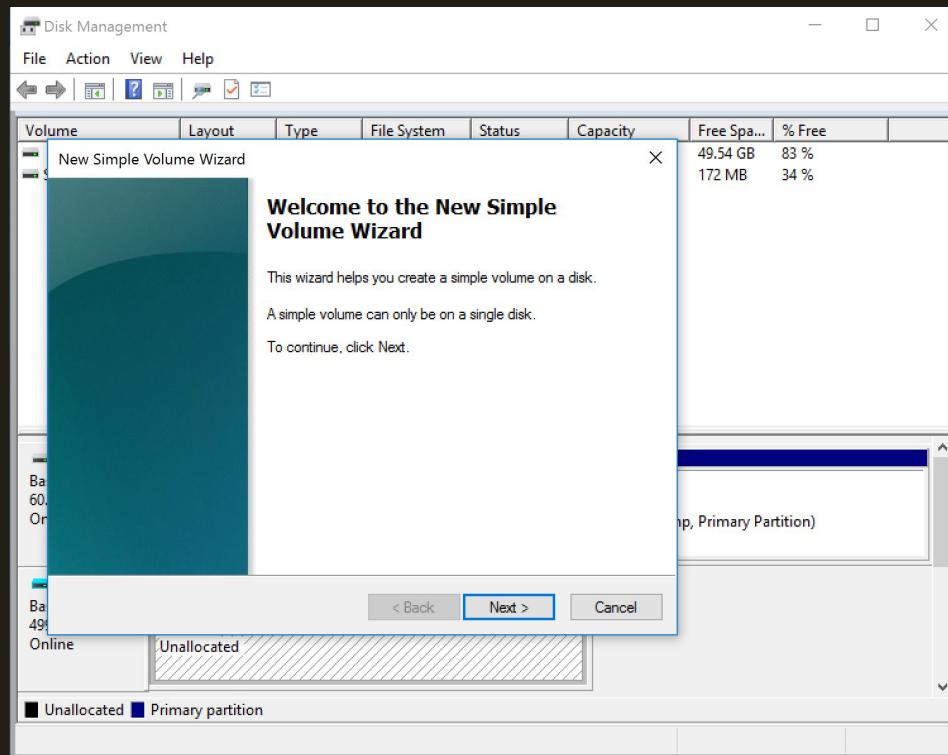
Step Two: Choose “Action » Create VHD”
to create a virtual hard disk

Practical file encryption (Windows)



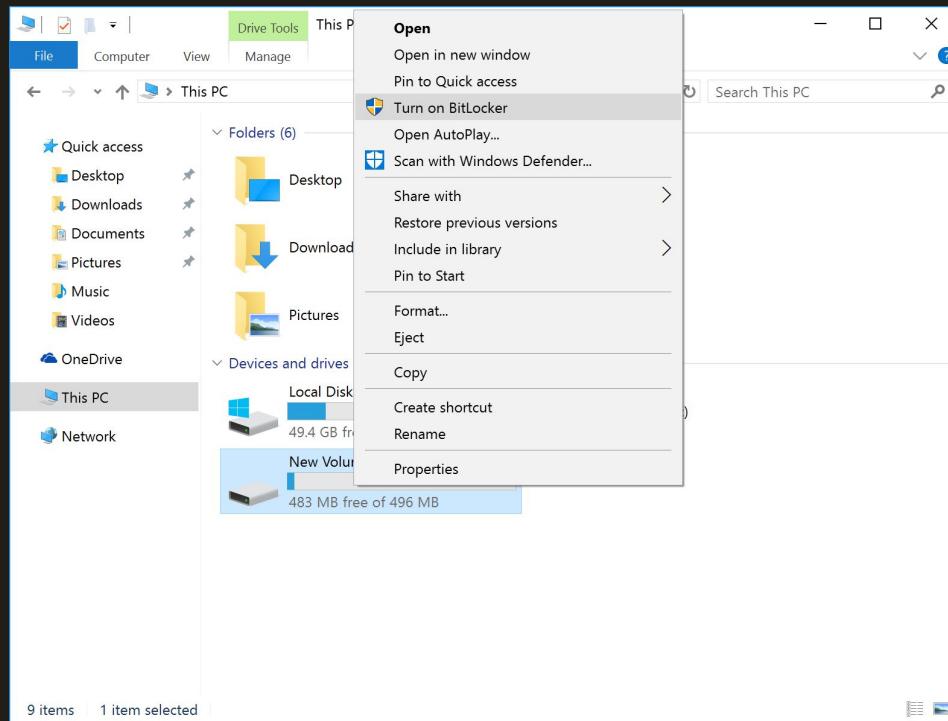
Step Three: Right click on the new disk and choose to “initialize disk”

Practical file encryption (Windows)



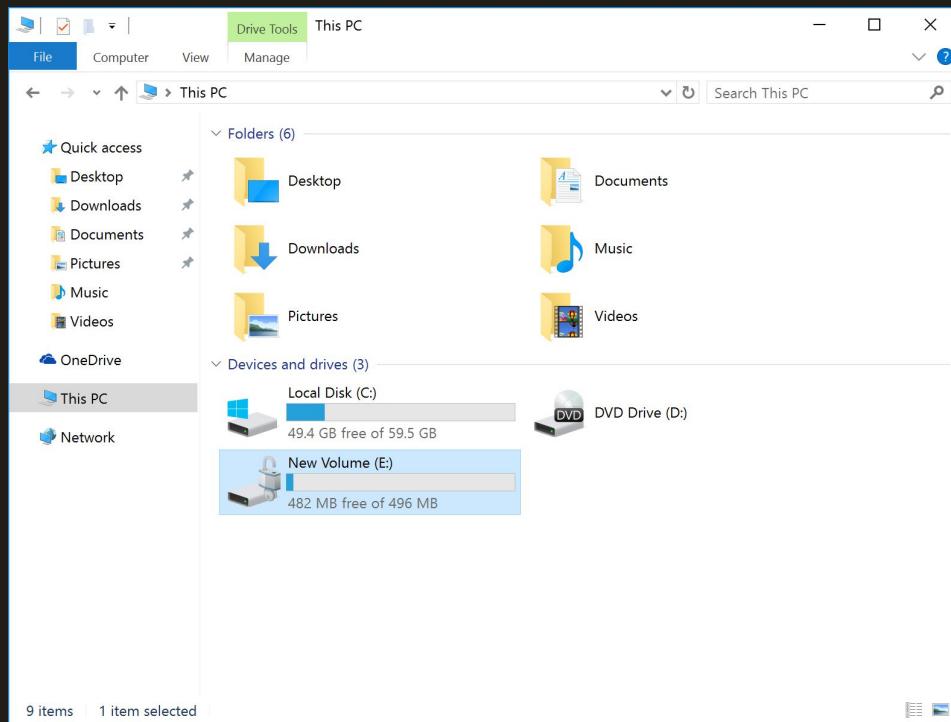
Step Four: Right click on the unallocated space and choose “New Simple Volume...”, then click “Next” four times followed by “Finish”

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!



Credit to Frank Chen

<https://kfrankc.me/cs88s/>