

7.1 Review CVEs and Buffer Overflows

Enter buffer overflow in keyword search

The screenshot shows the CVE Search List page at http://cve.mitre.org/cve/search_cve_list.html. The search bar at the top contains the text "buffer overflow". Below the search bar, there is a heading "Search Results" followed by a table with columns for "ID", "Title", "Published", "Last Modified", and "CVSS Score". The table lists several entries, with the first few being:

ID	Title	Published	Last Modified	CVSS Score
CVE-2017-1000001	Microsoft Windows Kernel Driver Memory Corruption	2017-01-10	2017-01-10	10.0
CVE-2017-1000002	Microsoft Windows Kernel Driver Memory Corruption	2017-01-10	2017-01-10	10.0
CVE-2017-1000003	Microsoft Windows Kernel Driver Memory Corruption	2017-01-10	2017-01-10	10.0
CVE-2017-1000004	Microsoft Windows Kernel Driver Memory Corruption	2017-01-10	2017-01-10	10.0
CVE-2017-1000005	Microsoft Windows Kernel Driver Memory Corruption	2017-01-10	2017-01-10	10.0

At the bottom of the page, there is a footer with links to "Contact Us", "Terms of Use", "Privacy Policy", "Site Map", "Search this Site", and "Follow CVE". There is also a link to "MITRE Corporation". The footer also includes copyright information and a "Page Last Updated or Reviewed" date of December 15, 2017.

Search Results

Screenshot of the CVE Search Results page on the MITRE website (<http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=buffer+overfl>) showing search results for "buffer+overfl".

The page displays 9532 matching CVE entries. The results are presented in a table with columns for Name and Description.

Name	Description
CVE-2018-9264	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the ADB dissector could crash with a heap-based buffer overflow. This was addressed in epan/dissectors/packet-adb.c by checking for a length inconsistency.
CVE-2018-9261	In Wireshark 2.0.0 to 2.4.5 and 2.2.0 to 2.2.13, the NBAP dissector could crash with a large loop that ends with a heap-based buffer overflow. This was addressed in epan/dissectors/packet-nbap.c by prohibiting the selflinking of DCH-IDs.
CVE-2018-9139	On Samsung mobile devices with N(7.x) software, a buffer overflow in the vision service allows code execution in a privileged process via a large frame size, aka SVE-2017-11165.
CVE-2018-9128	DVD X Player Standard 5.5.3.9 has a Buffer Overflow via a crafted .plf file, a related issue to CVE-2007-3068.
CVE-2018-9063	MapDrv (C:\Program Files\Lenovo\System Update\mapdrv.exe) In Lenovo System Update versions earlier than 5.07.0072 contains a local vulnerability where an attacker entering very large user ID or password can overrun the program's buffer, causing undefined behaviors, such as execution of arbitrary code. No additional privilege is granted to the attacker beyond what is already possessed to run MapDrv.
CVE-2018-9059	Stack-based buffer overflow in Easy File Sharing (EFS) Web Server 7.2 allows remote attackers to execute arbitrary code via a malicious login request to forum.ghp. NOTE: this may overlap CVE-2014-3791.
CVE-2018-8941	Diagnostics functionality on D-Link DSL-3782 devices with firmware EU v. 1.01 has a buffer overflow, allowing authenticated remote attackers to execute arbitrary code via a long Addr value to the 'set Diagnostics_Entry' function in an HTTP request, related to /users/bin/tcpip.
CVE-2018-8905	In LIBTIFF 4.0.9, a heap-based buffer overflow occurs in the function LZWDecodeCompat in tif_lzw.c via a crafted TIFF file, as demonstrated by tiff2ps.
CVE-2018-8871	In Delta Electronics Automation TPEditor version 1.89 or prior, parsing a malformed program file may cause heap-based buffer overflow vulnerability, which may allow remote code execution.
CVE-2003-0575	Heap-based buffer overflow in the name services daemon (nsd) in SGI IRIX 6.5.x through 6.5.21f, and possibly earlier versions, allows attackers to gain root privileges via the AUTH_UNIX gid list.
CVE-2003-0562	Buffer overflow in the CGI2PERL.NLM PERL handler in Novell Netware 5.1 and 6.0 allows remote attackers to cause a denial of service (ABEND) via a long input string.
CVE-2003-0561	Multiple buffer overflows in IglooFTP PRO 3.8 allow remote FTP servers to execute arbitrary code via (1) a long FTP banner, or long responses to the client commands (2) USER, (3) PASS, (4) ACCT, and possibly other commands.
CVE-2003-0558	Buffer overflow in LeapFTP 2.7.3.600 allows remote FTP servers to execute arbitrary code via a long IP address response to a PASV request.
CVE-2003-0553	Buffer overflow in the Client Detection Tool (CDT) plugin (npcd.dll) for Netscape 7.02 allows remote attackers to execute arbitrary code via an attachment with a long filename.
CVE-2003-0542	Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache before 1.3.29 allow attackers to create configuration files to cause a denial of service (crash) or execute arbitrary code via a regular expression with more than 9 captures.
CVE-2003-0535	Buffer overflow in xl1 1.0k and earlier allows local users to gain privileges via a long -display command line option.
CVE-2003-0533	Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPRMOCO.LOG log file, as exploited by the Sasser worm.
CVE-2003-0530	Buffer overflow in the BR549.DLL ActiveX control for Internet Explorer 5.01 SP3 through 6.0 SP1 allows remote attackers to execute arbitrary code.
CVE-2003-0528	Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed RPC request with a long filenam parameter, a different vulnerability than CVE-2003-0352 (Blaster/Nachi) and CVE-2003-0715.
CVE-2003-0518	The screen saver in Mac OS X allows users with physical access to cause the screen saver to crash and gain access to the underlying session via a large number of characters in the password field, possibly triggering a buffer overflow.
CVE-2003-0508	Buffer overflow in the WWWLaunchNetscape function of Adobe Acrobat Reader (acroread) 5.0.7 and earlier allows remote attackers to execute arbitrary code via a .pdf file with a long mailto link.
CVE-2003-0507	Stack-based buffer overflow in Active Directory in Windows 2000 before SP4 allows remote attackers to cause a denial of service (reboot) and possibly execute arbitrary code via an LDAP version 3 search request with a large number of (1) "AND," (2) "OR," and possibly other statements, which causes LSASS.EXE to crash.
CVE-2003-0503	Buffer overflow in the ShellExecute API function of SHELL32.DLL in Windows 2000 before SP4 may allow attackers to cause a denial of service or execute arbitrary code via a long third argument.
CVE-2003-0488	Multiple cross-site scripting (XSS) vulnerabilities in Kerio MailServer 5.6.3 allow remote attackers to insert arbitrary web script via (1) the add_name parameter in the add_acl module, or (2) the alias parameter in the do_map module.
CVE-2003-0487	Multiple buffer overflows in Kerio MailServer 5.6.3 allow remote authenticated users to cause a denial of service and possibly execute arbitrary code via (1) a long showuser parameter in the do_subscribe module, (2) a long folder parameter in the add_acl module, (3) a long folder parameter in the list module, and (4) a long user parameter in the do_map module.
CVE-2003-0485	Buffer overflow in Progress 4GL Compiler 9.1D06 and earlier allows attackers to execute arbitrary code via source code containing a long, invalid data type.

The worm that exploited CVE-2003-0553 is the Sasser Worm.

CVE-2003-0533 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPROMO.LOG log file, as exploited by the Sasser worm.

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- FULLDISC:20040413 EEYE: Windows Local Security Authority Service Remote Buffer Overflow
- URL:<http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>
- EEYE:AD20040413C
- URL:<http://www.eeye.com/html/Research/Advisories/AD20040413C.html>
- BUGTRAQ:20040429 MS04011 Lsassrv.dll RPC buffer overflow remote exploit (PoC)
- URL:<http://marc.info/?l=bugtraq&m=108325860431471&w=2>
- MS:MS04-011
- URL:<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2004/ms04-011>
- CERT:TA04-104A
- URL:<http://www.us-cert.gov/cas/techalerts/TA04-104A.html>
- CERT-VN:VN#753212
- URL:<http://www.kb.cert.org/vuls/id/753212>
- CIAC:O-114
- URL:<http://www.ciac.org/ciac/bulletins/o-114.shtml>
- BID:10108
- URL:<http://www.securityfocus.com/bid/10108>
- OVAL:oval:org.mitre.oval:def:883
- URL:https://oval.cisecurity.org/repository/search/definition/oval%3Aorg_mitre_oval%3Adef%3A883
- OVAL:oval:org.mitre.oval:def:898

Search for CVE-2016-6444

CVE - Search CVE List Go to for: CVSS Scores CPE Info Advanced Search

Common Vulnerabilities and Exposures

Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

TOTAL CVE Entries: 108202

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a [CVE Entry](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Entries.

View the [search tips](#).

Page Last Updated or Reviewed: December 15, 2017

CSRF

Screenshot of the CVE Search Results page on the MITRE website.

The page shows a search result for CVE-2016-6444, which details a vulnerability in Cisco Meeting Server related to CSRF attacks.

Search Results
There are 1 CVE entries that match your search.

Name	Description
CVE-2016-6444	A vulnerability in Cisco Meeting Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a Web Bridge user. More Information: CSCvb03308. Known Affected Releases: 1.8, 1.9, 2.0.

SEARCH CVE USING KEYWORDS:
You can also search by reference using the [CVE Reference Maps](#).
For More Information: cve@mitre.org

CVE-ID
CVE-2016-6444 [Learn more at National Vulnerability Database \(NVD\)](#)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
A vulnerability in Cisco Meeting Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a Web Bridge user. More Information: CSCvb03308. Known Affected Releases: 1.8, 1.9, 2.0.

References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms>
- BID:[93785](#)
- URL:<http://www.securityfocus.com/bid/93785>

Assigning CNA
Cisco Systems, Inc.

Date Entry Created
20160726 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

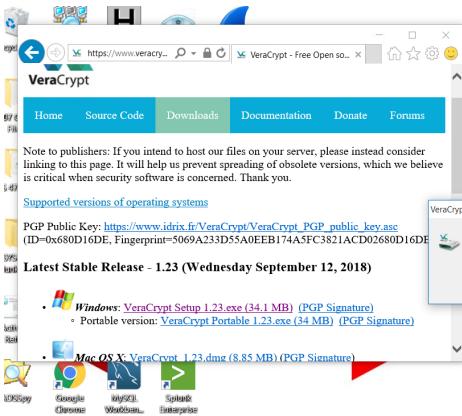
Phase (Legacy)
Assigned (20160726)

Votes (Legacy)

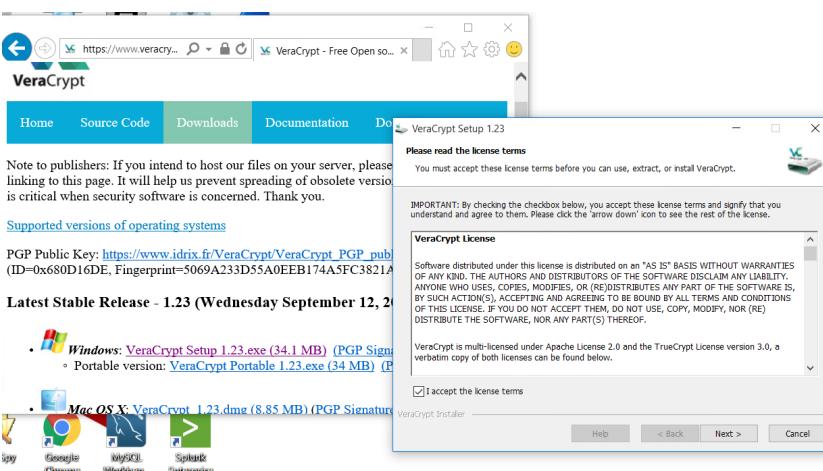
Comments (Legacy)

10.1 Encrypting Data at Rest for Added Physical Security

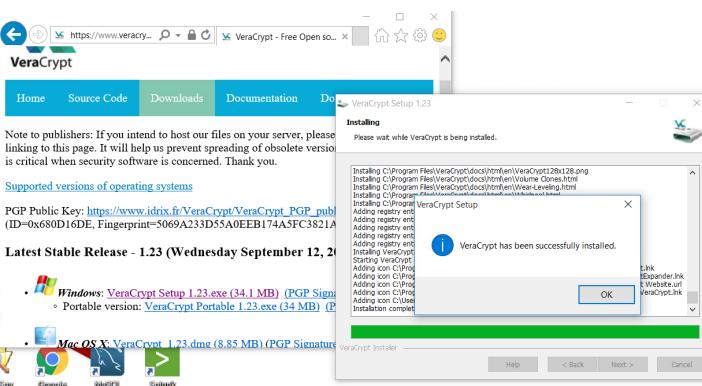
Download and install VeraCrypt



RYVILLE
UNIVERSITY

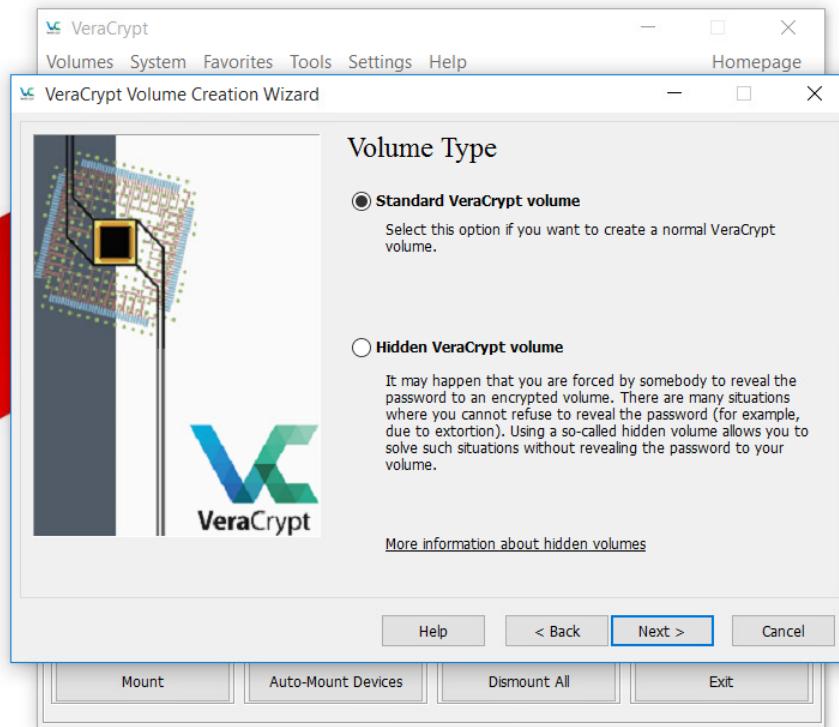
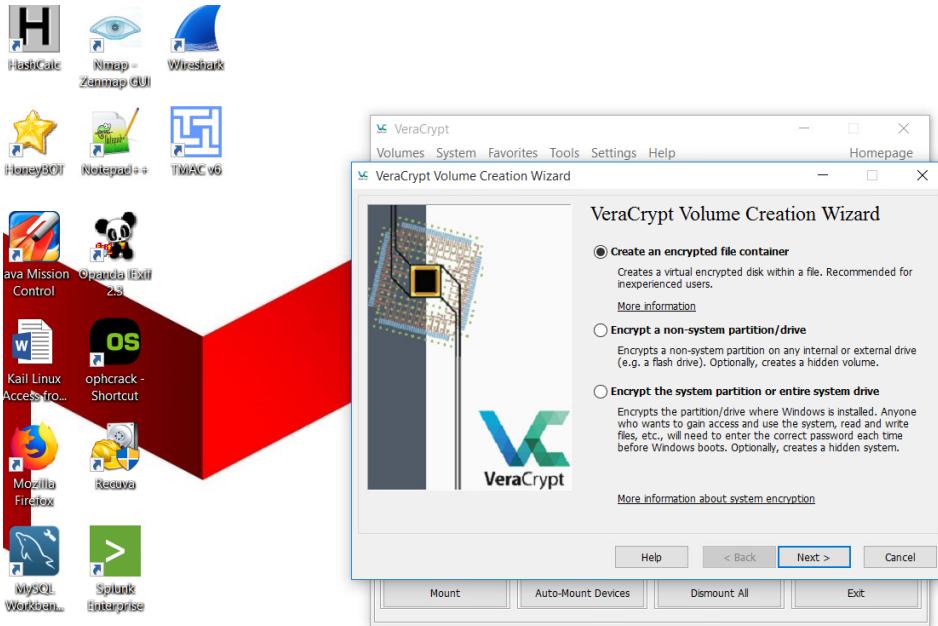


YVILLE
UNIVERSITY

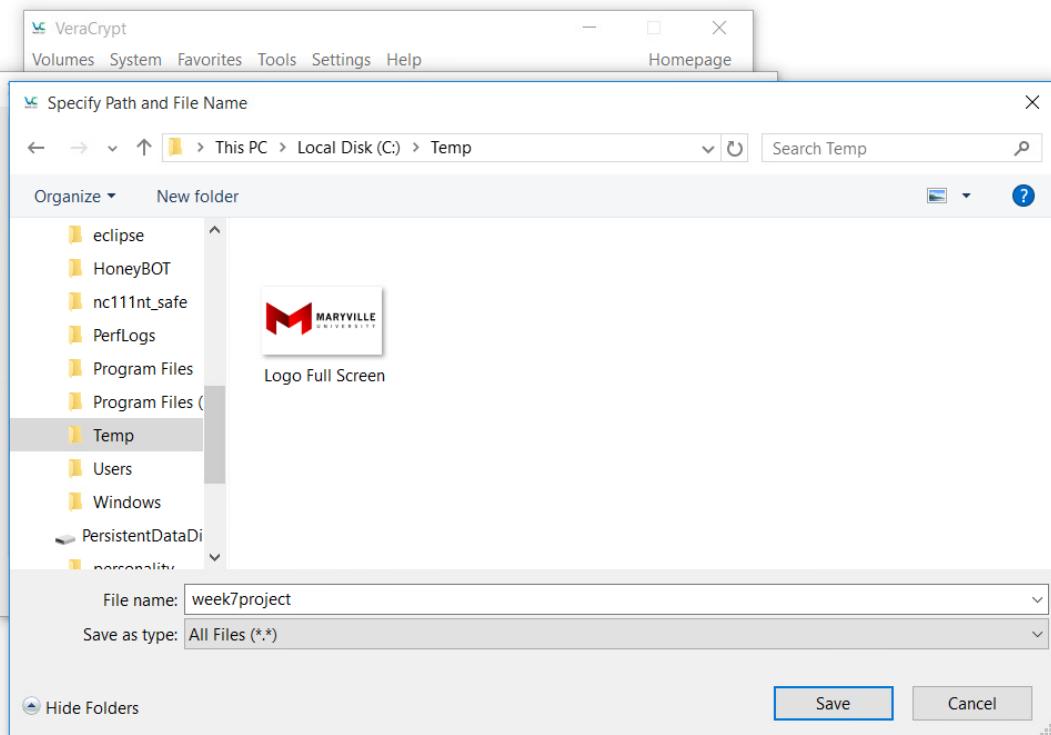


YVILLE
UNIVERSITY

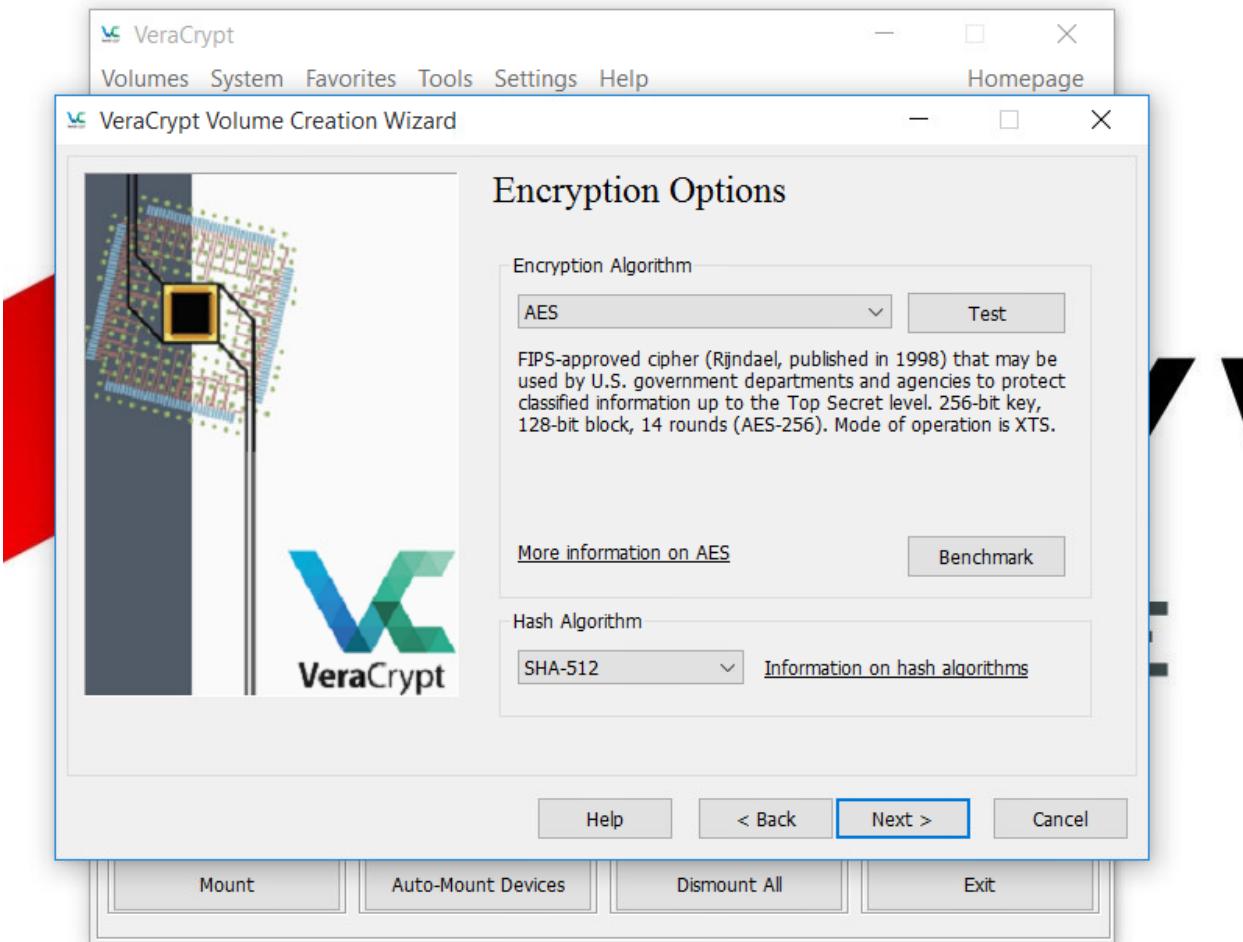
Create Volume



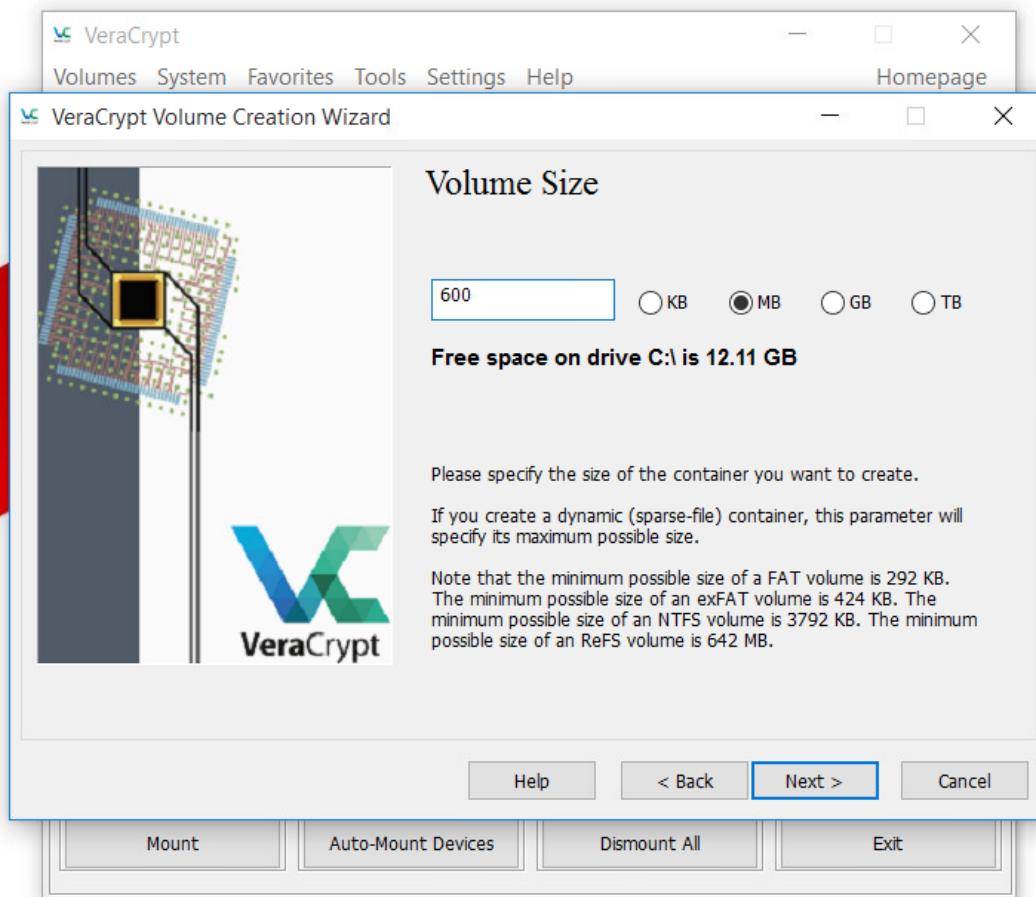
Choose location and Name file



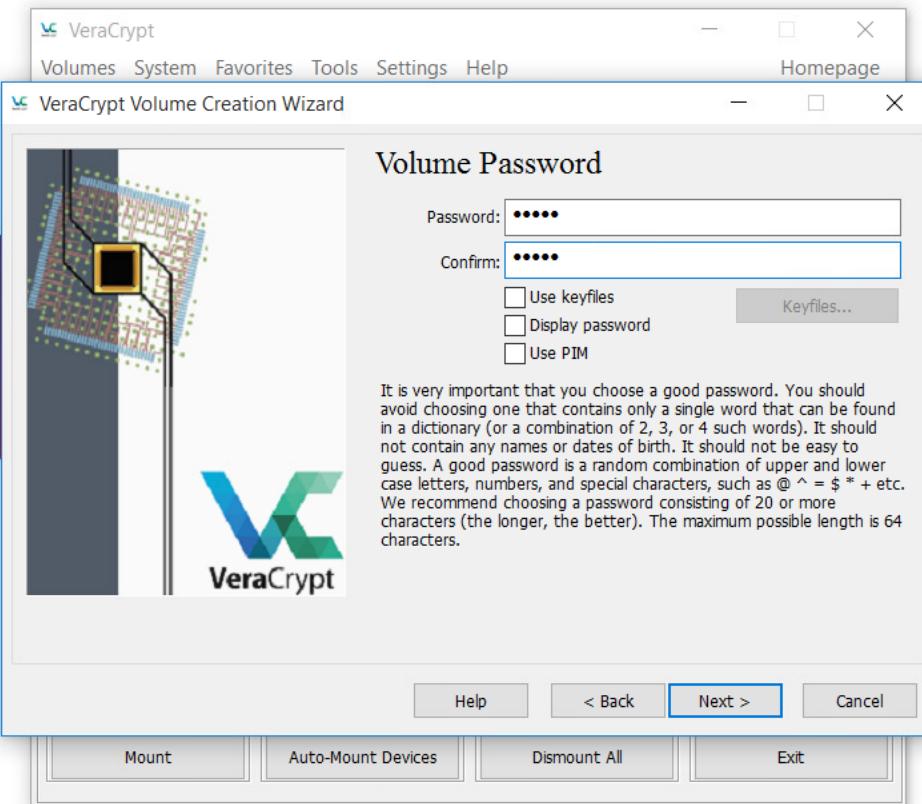
Default setting for encryption algorithm and hash logarithm for volume



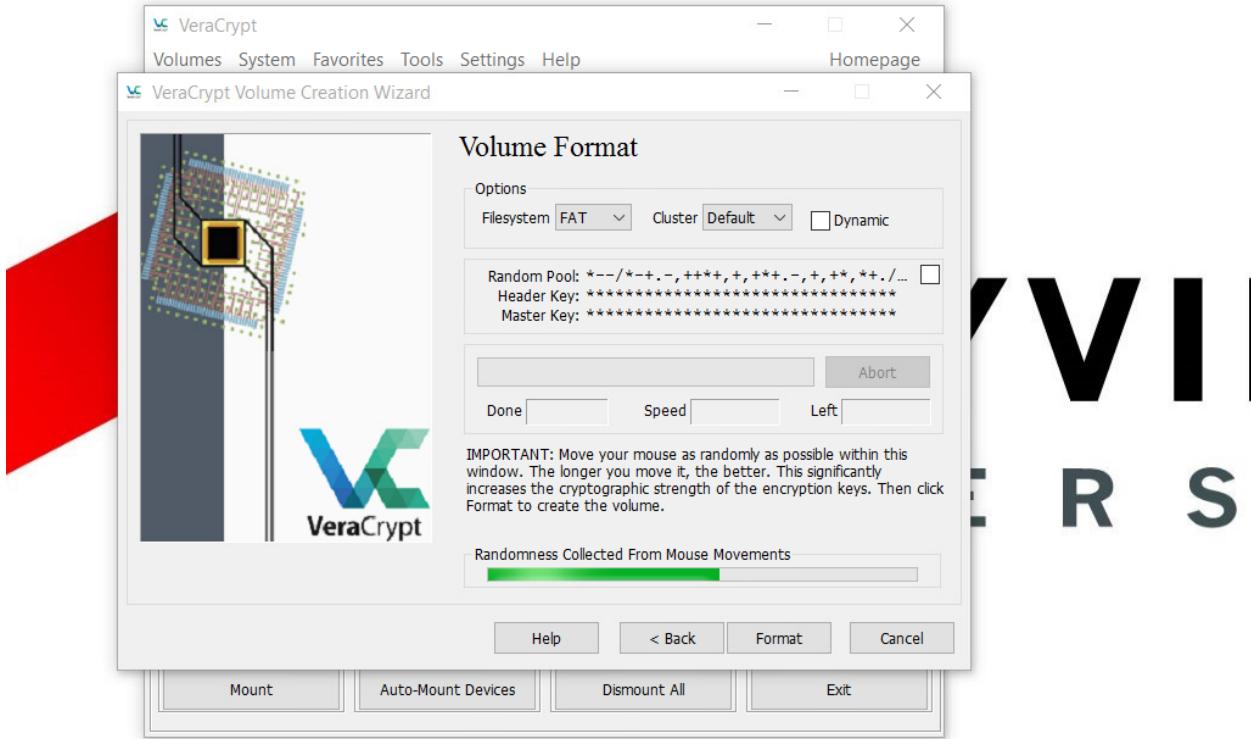
Specify size of VeraCrypt container



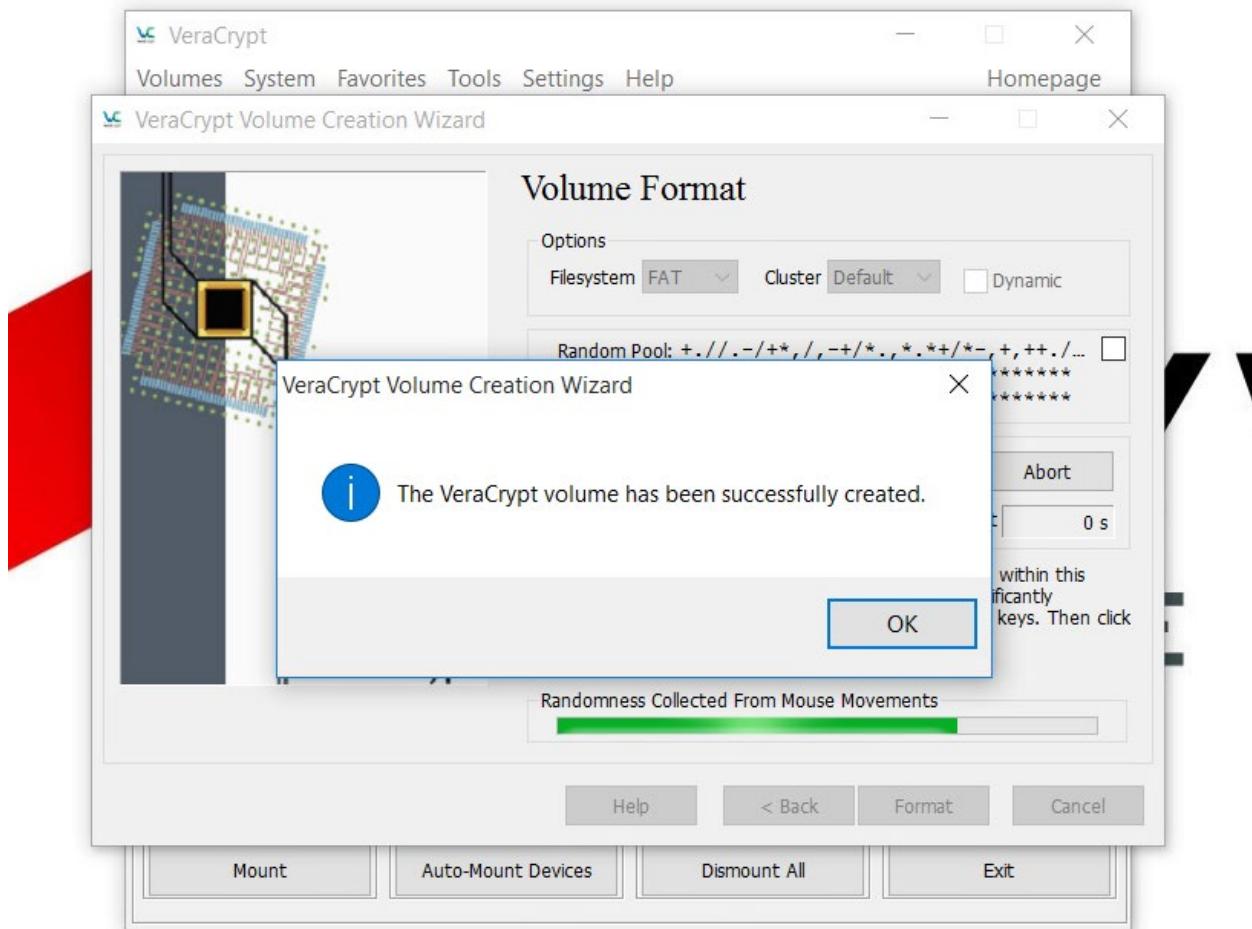
Create volume password

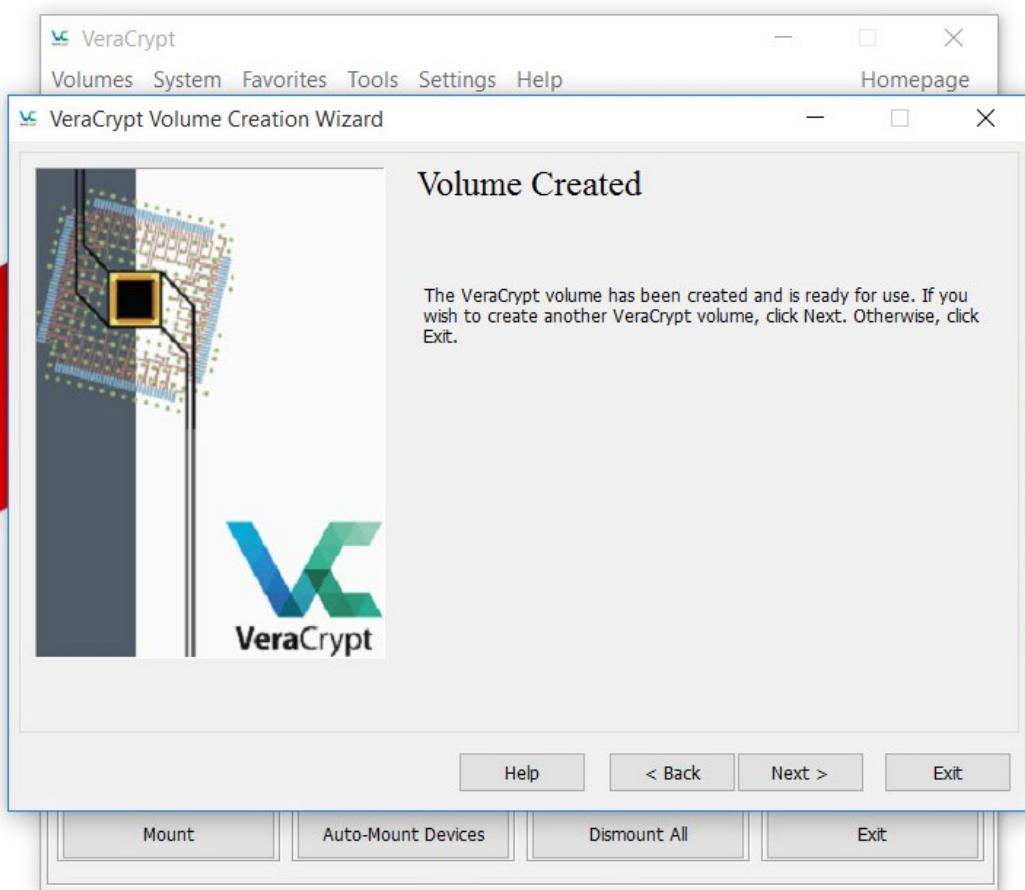


Move mouse around so that randomness indicator becomes green



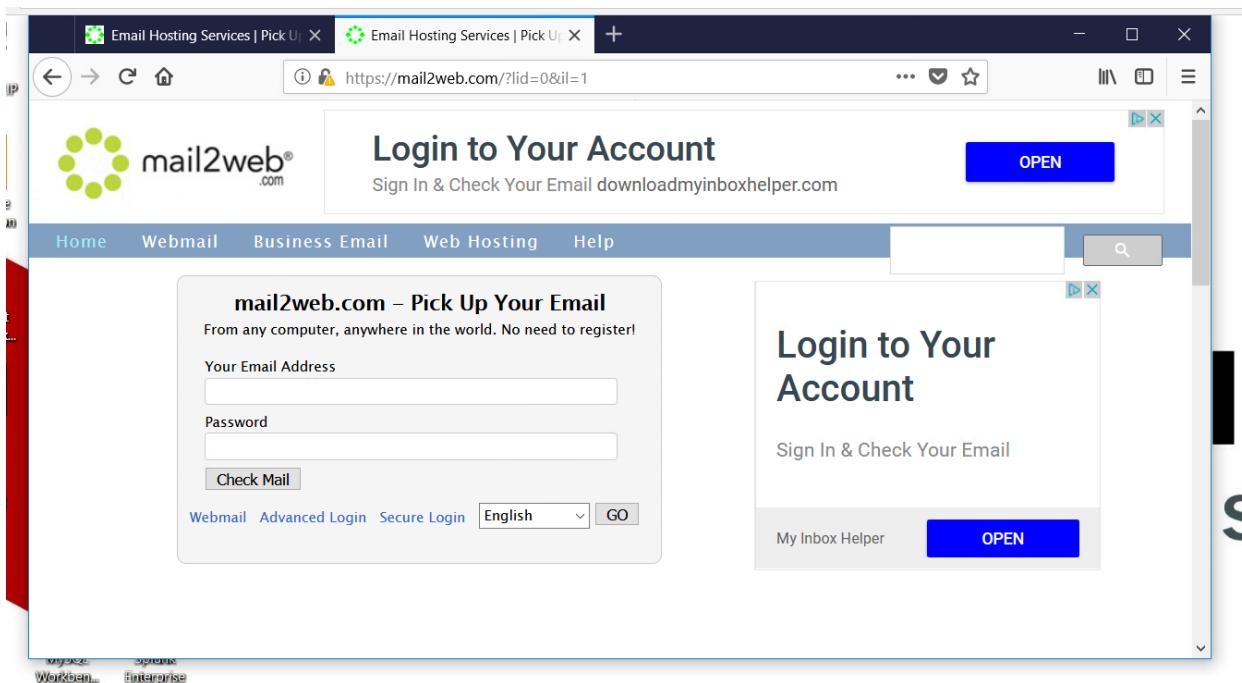
Confirmation that VeraCrypt volume has been successfully created.



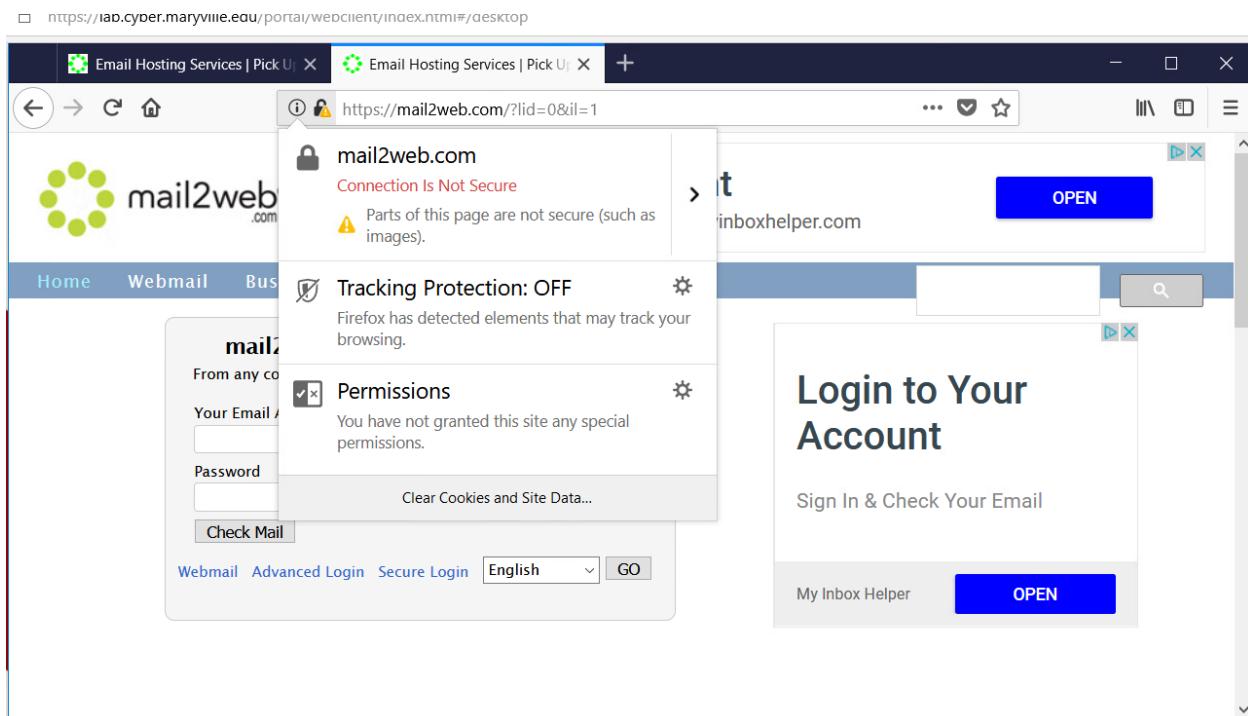


11.1 Examining an SSL Certificate

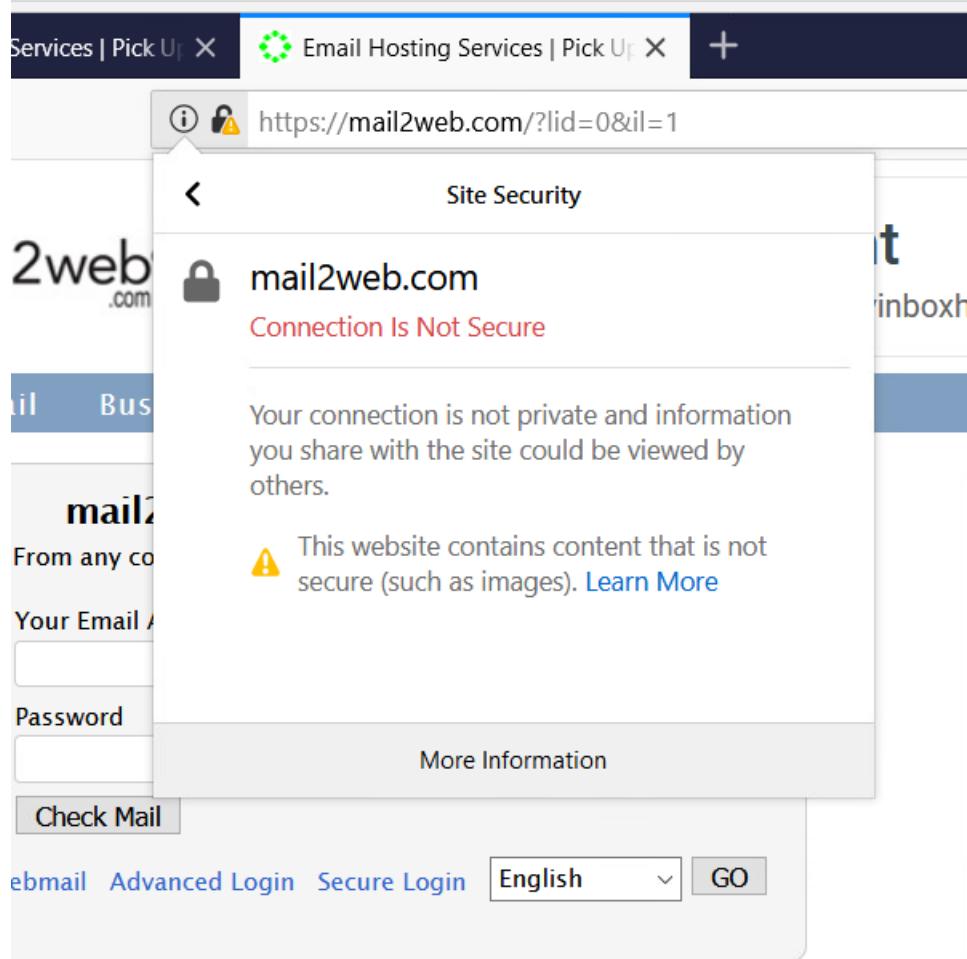
Go to mail2web.com and choose secure login option



Click SSL icon in the address bar



SSL icon information



More information from SSL icon in previous pic

Page Info - https://mail2web.com/?lid=0&il=1

General Media Permissions Security

Website Identity

Website: mail2web.com
Owner: This website does not supply ownership information.
Verified by: Not specified

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Partially Encrypted
Parts of the page you are viewing were not encrypted before being transmitted over the Internet.
Information sent over the Internet without encryption can be seen by other people while it is in transit.

[Help](#)

View certificate [general information]

Certificate Viewer: "www.mail2web.com" X

[General](#) [Details](#)

This certificate has been verified for the following uses:

SSL Client Certificate
SSL Server Certificate

Issued To

Common Name (CN) [www.mail2web.com](#)
Organization (O) Softcom Inc.
Organizational Unit (OU) Operations
Serial Number 00:84:A1:EC:B8:92:90:7F:D1:BA:4B:21:21:88:96:9B:2C

Issued By

Common Name (CN) COMODO RSA Organization Validation Secure Server CA
Organization (O) COMODO CA Limited
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity

Begins On Thursday, July 13, 2017
Expires On Thursday, July 18, 2019

Fingerprints

SHA-256 Fingerprint 40:37:32:25:2C:DC:6A:FF:A6:1F:47:0C:64:C2:96:7A:
83:3D:FE:00:F2:7F:4F:9D:5F:6C:58:40:50:89:D5:87
SHA1 Fingerprint D9:88:F2:E8:AA:A8:48:49:BB:77:B1:C7:36:CD:17:3F:C1:54:18:4B

[Close](#)

Details of certificate

Email | mail2web.com | Certificate viewer: www.mail2web.com" X

General Details

Certificate Hierarchy

- ✓ COMODO RSA Certification Authority
- ✓ COMODO RSA Organization Validation Secure Server CA
- www.mail2web.com

Certificate Fields

- ✓ www.mail2web.com
 - ✓ Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - ✓ Validity
 - Not Before

Field Value

Export...

Close

[General](#) [Details](#)**This certificate has been verified for the following uses:****SSL Client Certificate****SSL Server Certificate****Issued To**

Common Name (CN) www.mail2web.com
Organization (O) Softcom Inc.
Organizational Unit (OU) Operations
Serial Number 00:84:A1:EC:B8:92:90:7F:D1:BA:4B:21:21:88:96:9B:2C

Issued By

Common Name (CN) COMODO RSA Organization Validation Secure Server CA
Organization (O) COMODO CA Limited
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity

Begins On Thursday, July 13, 2017
Expires On Thursday, July 18, 2019

Fingerprints

SHA-256 Fingerprint 40:37:32:25:2C:DC:6A:FF:A6:1F:47:0C:64:C2:96:7A:
83:3D:FE:00:F2:7F:4F:9D:5F:6C:58:40:50:89:D5:87
SHA1 Fingerprint D9:88:F2:E8:AA:A8:48:49:BB:77:B1:C7:36:CD:17:3F:C1:54:18:4B

Certificate expires July 18th, 2019

[Close](#)

Certificate Signature Algorithm

Certificate Signature Value

field Value

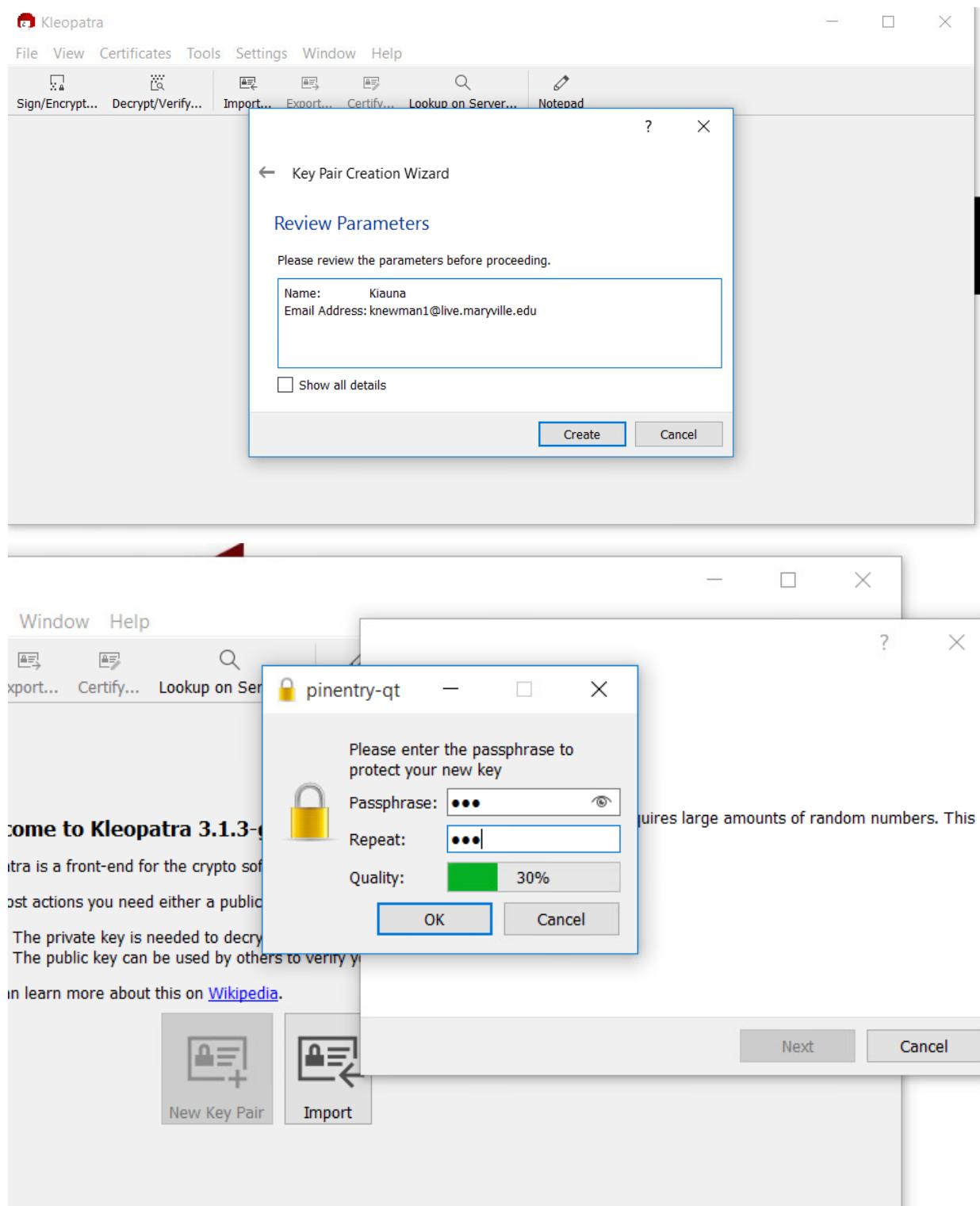
PKCS #1 SHA-256 With RSA Encryption

SHA-256 was used sign the certifitcate

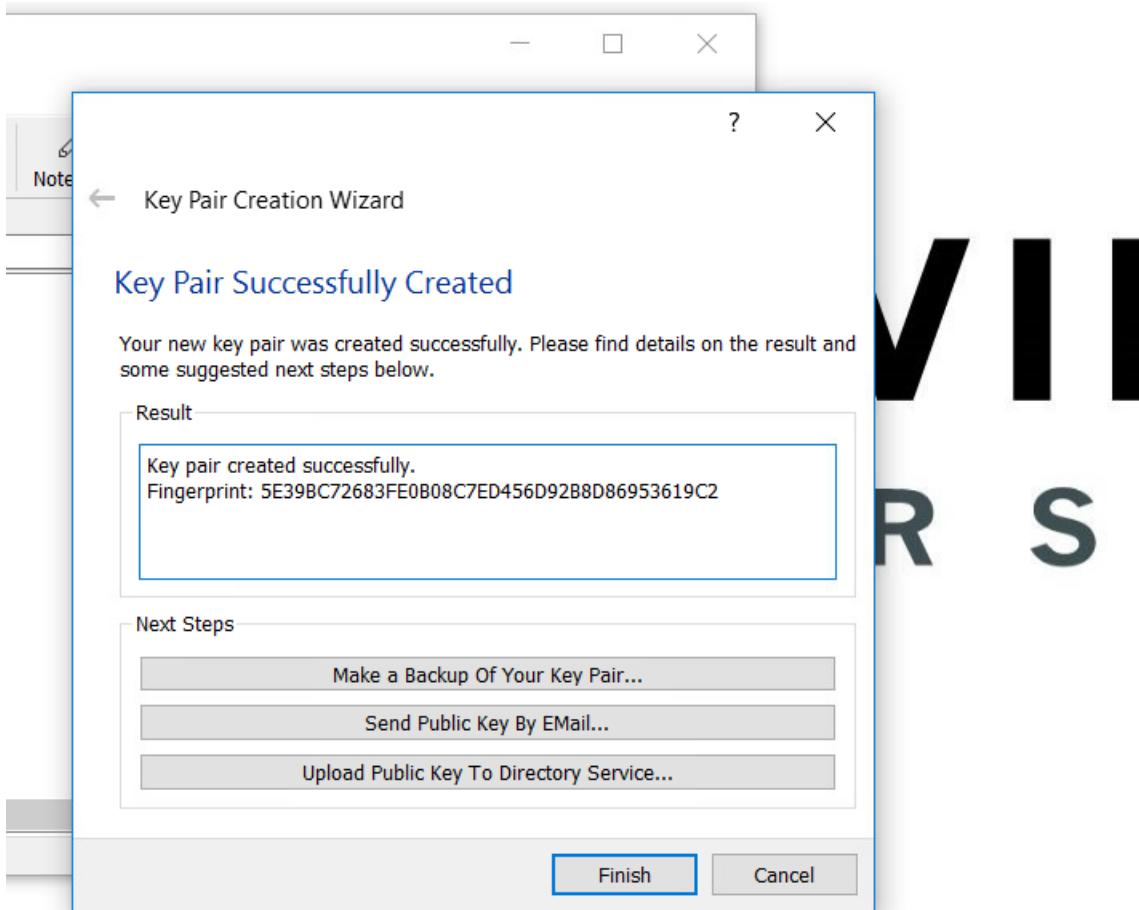
Deliverables

1. Using GPG for Encryption

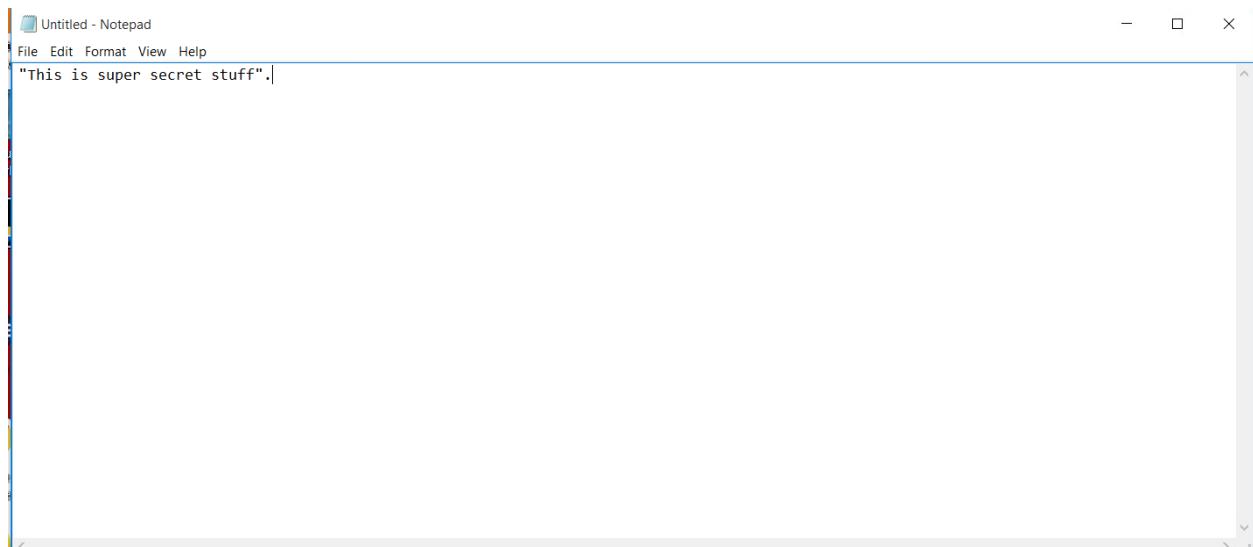
Run Kleopatra to create a New Key Pair.



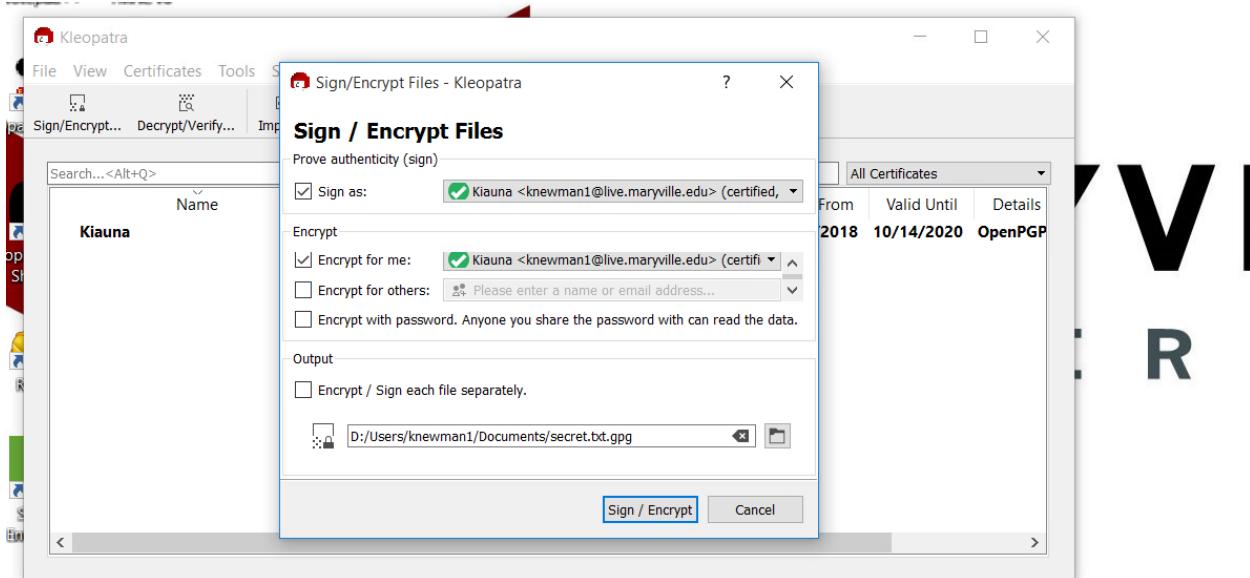
Confirmation that creation of keypair was sucessful



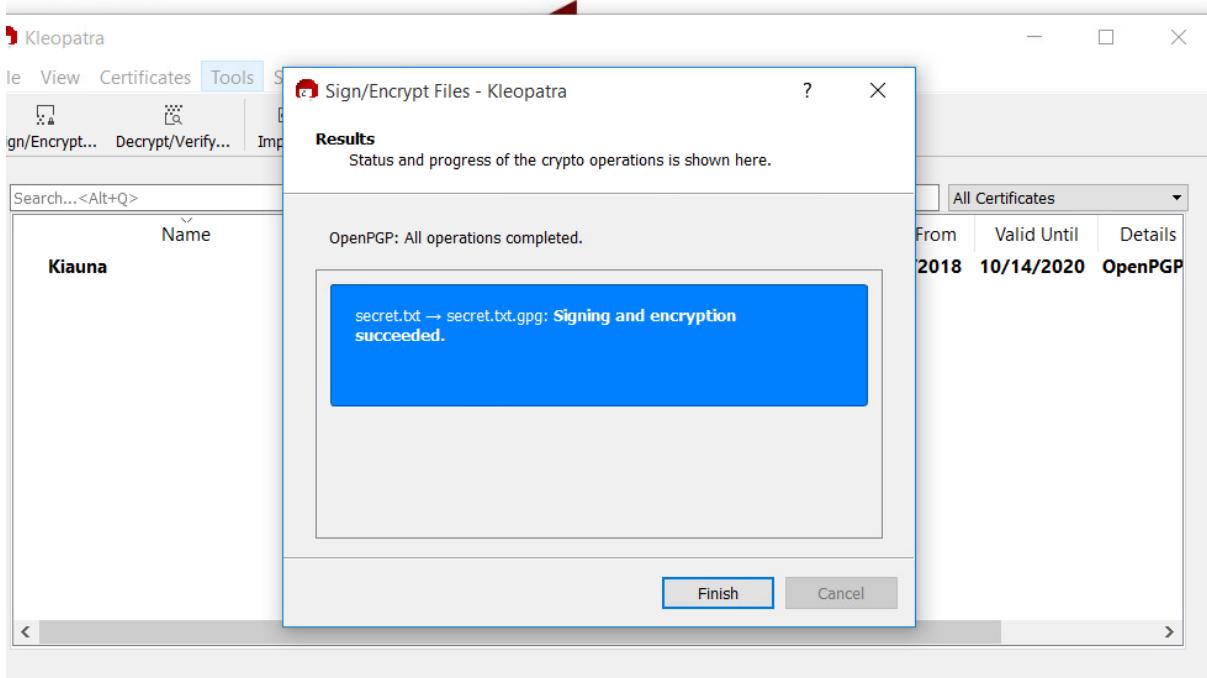
Open Notepad and create a `secret.txt` file with the text `This is super secret stuff` inside the file.



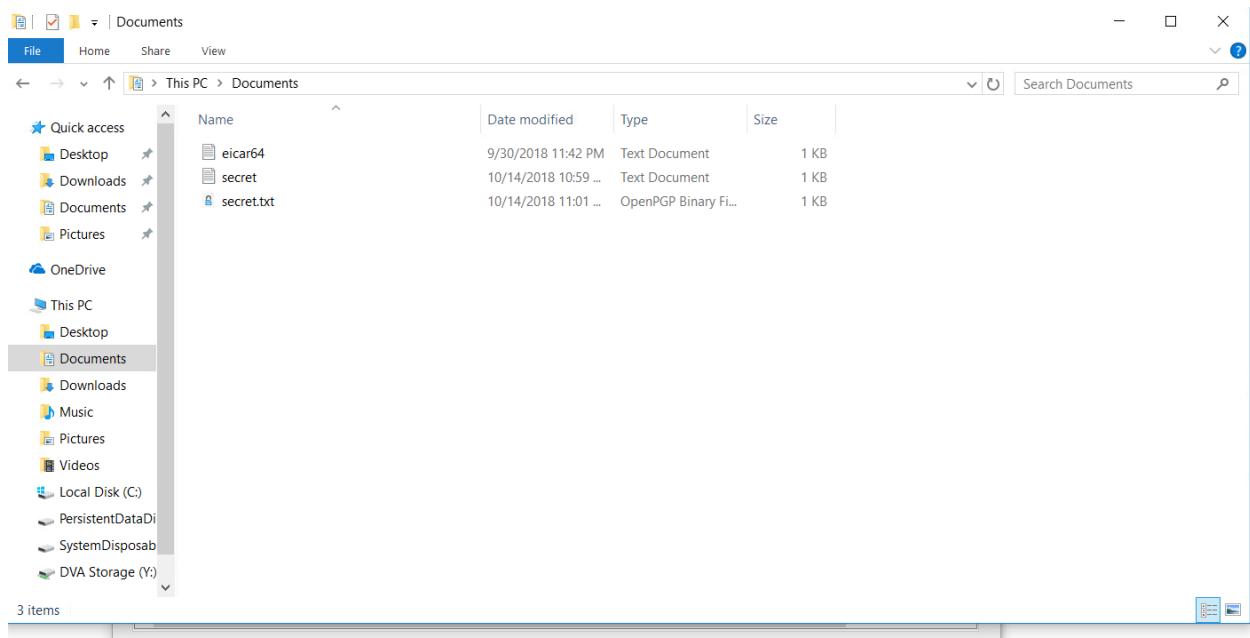
Click on Sign Encrypt in Kleopatra and encrypt the secret.txt file.



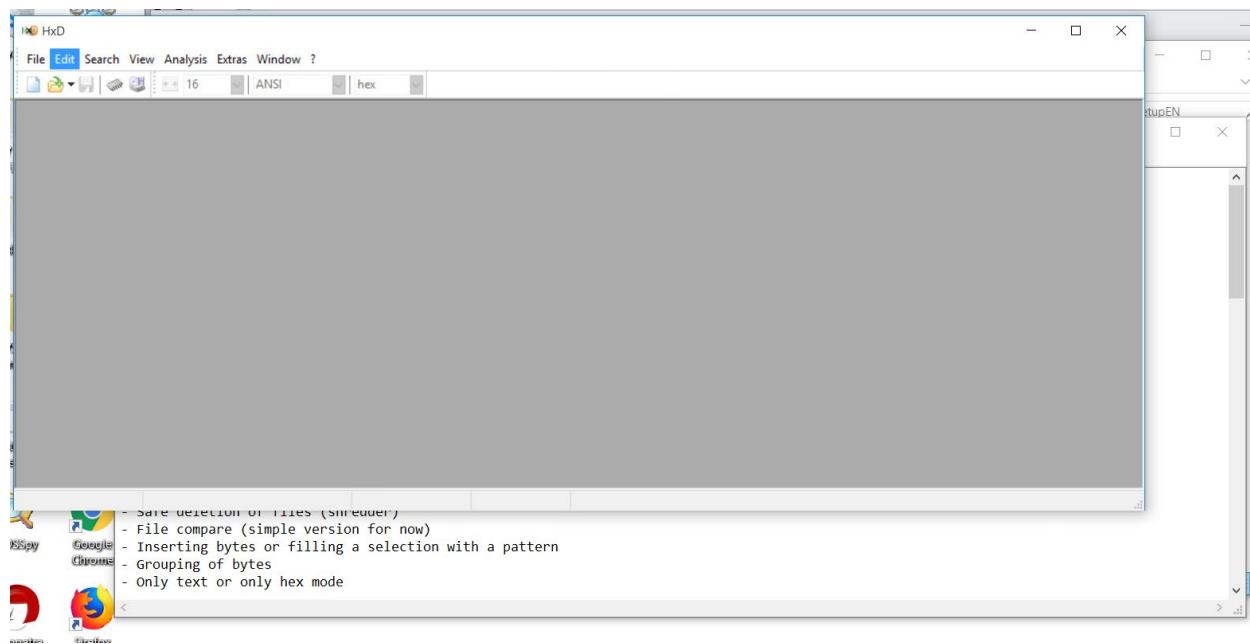
Completion of signing and encryption



Screen-shot of secret.txt file and secret.txt.gpg file



Opening HxD editor



view the secret.txt.gpg file and the secret.txt file.

The image shows two side-by-side hex editors, both titled "secret.txt.gpg".

The top window displays the raw binary data of the file. The bottom window shows the decrypted version of the file, with the title bar indicating "decrypted version as n0secret.txt".

Both windows have a toolbar at the top with icons for File, Edit, Search, View, Analysis, Extras, Window, and Help. The menu bar includes File, Edit, Search, View, Analysis, Extras, Window, and ?.

The left pane of each window lists file offsets from 00000000 to 00000140. The right pane shows the corresponding hex values and ASCII characters.

In the top window, the ASCII data includes the string "This is super s" followed by "ecret stuff".

In the bottom window, the ASCII data is mostly illegible due to decryption, showing various characters and symbols.

Offset (h)	secret.txt.gpg (Raw)	secret.txt.gpg (Decrypted)
00000000	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	00 01 0C 03 E0 C3 60 E0 EC 18 2F 10 01 08 00 DE
00000010	B2 54 68 69 73 20 69 73 20 73 75 70 65 72 20 73	B2 54 68 69 73 20 69 73 20 73 75 70 65 72 20 73
00000020	65 63 72 65 74 20 73 74 75 66 66 22 2E	65 63 72 65 74 20 73 74 75 66 66 22 2E
00000030	This is super s	This is super s
00000040	ecret stuff".	ecret stuff".

Is there any clear text in the secret.txt.gpg file

There isn't any clear text in the gpg file.

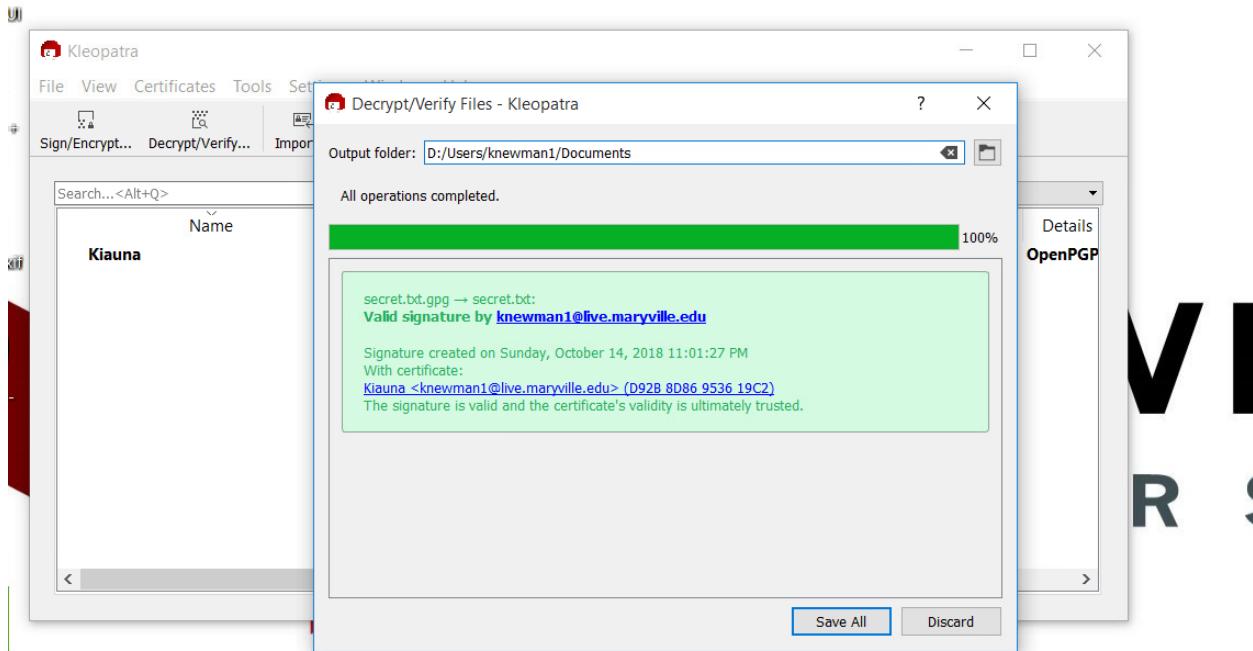
What about the secret.txt file

The phrase "this is super secret stuff" is shown.

Did you successfully encrypt the file

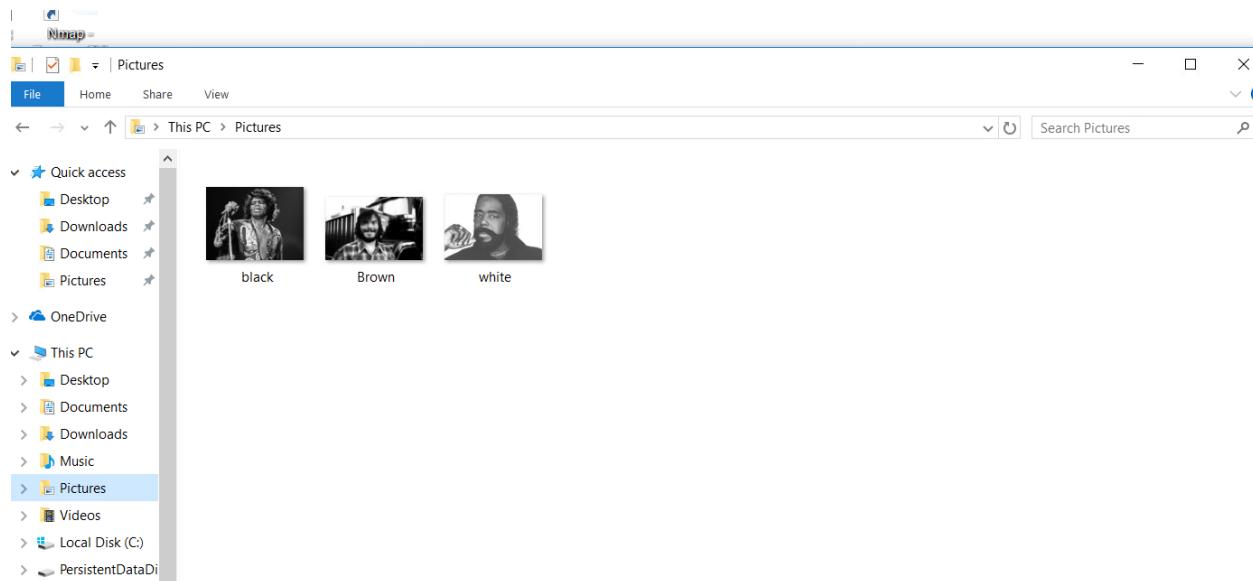
yes

Decrypt secret.txt.gpg



2. MD5 Hash Collisions

Download the three images and save as Black, Brown, and White.

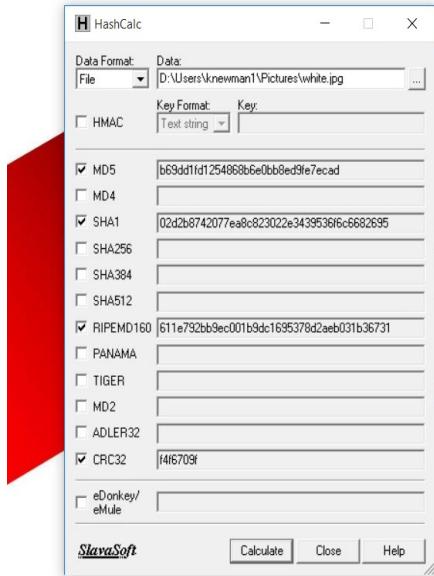
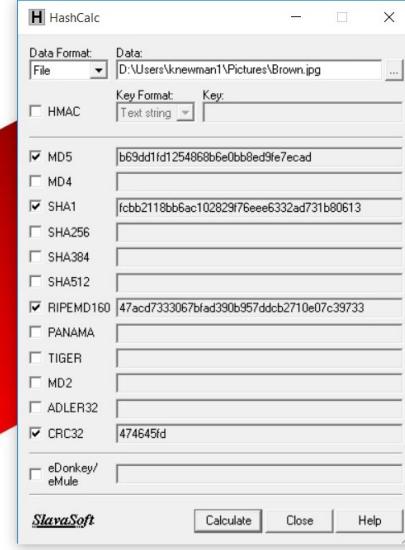
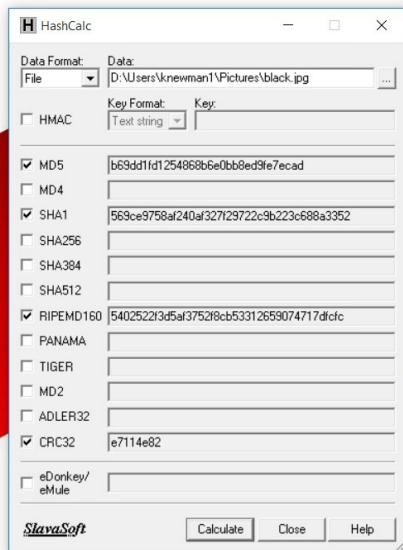


Use HashCalc (should be on the VM Desktop) to determine the MD5 and SHA1 message digests for each of the three images downloaded.

Black.jpg

Brown.jpg

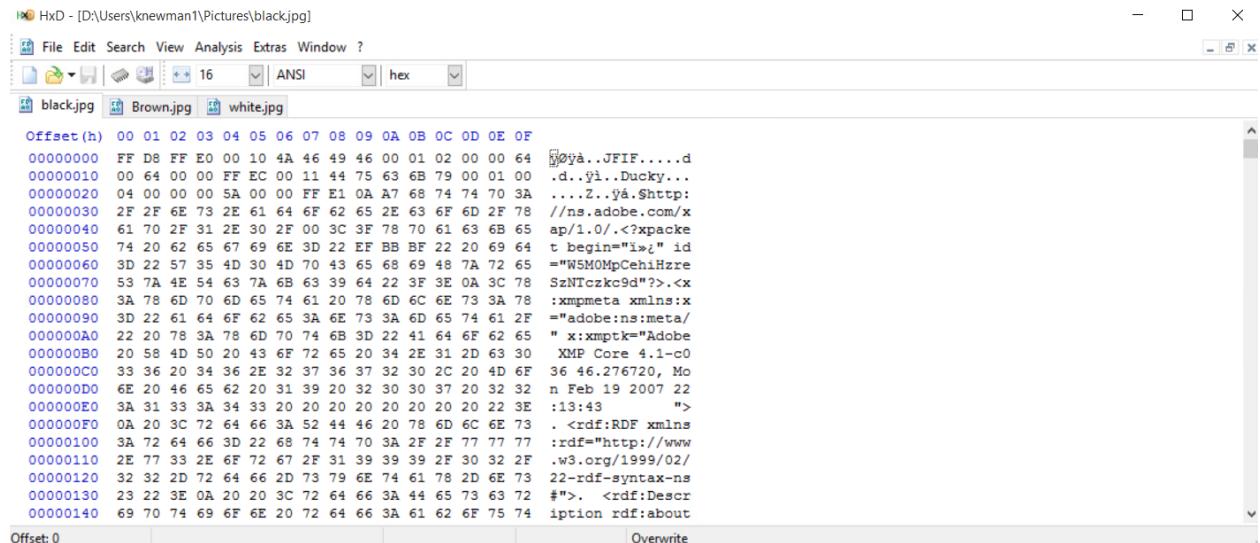
White.jpg



What is this an example of?

When all of the images have the same MD5, that is an example of a hash collision

Open each image with HxD and look at the jpg header data.



The screenshot shows the HxD hex editor interface with the file 'black.jpg' loaded. The menu bar is visible at the top, and the main window displays the file's contents in a hex dump format. The dump shows the standard JPEG file structure, including the SOI (Start Of Image) marker (FF D8 FF E0 00 10), the JFIF header, and various other metadata and data segments. The ASCII pane below the dump shows the corresponding characters for each byte. The status bar at the bottom indicates 'Offset: 0' and 'Overwrite'.

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 64 Moya..JFIF.....d
00 64 00 00 FF EC 00 11 44 75 63 6B 79 00 01 00 .d..ÿi..Ducky...
00 00 00 20 04 00 00 5A 00 00 FF E1 0A A7 68 74 74 70 3A ...Z..ÿA.$http:
00 00 00 30 2F 2E 73 2E 61 64 6F 62 65 2E 63 6F 6D 2F 78 //ns.adobe.com/x
00 00 00 40 61 70 2F 31 2E 30 2F 00 3C 3F 78 70 61 63 6B 65 ap/1.0./<?xpacke
00 00 00 50 74 20 62 65 67 69 6E 3D 22 EF BB BF 22 20 69 64 t begin="i>" id
00 00 00 60 3D 22 57 35 4D 30 4D 70 43 65 68 69 48 7A 72 65 ="W5M0MpCeHHzre
00 00 00 70 53 7A 4E 54 63 7A 6B 63 39 64 22 3F 3E 0A 3C 78 SzNTczkc9d">.<x
00 00 00 80 3A 78 6D 70 6D 65 74 61 20 78 6D 6C 6E 73 3A 78 :xmpmeta xmlns:x
00 00 00 90 3D 22 61 64 6F 62 65 3A 6E 73 3A 6D 65 74 61 2F ="adobe:ns:meta/
00 00 00 A0 22 20 78 3A 78 6D 70 74 6B 3D 22 41 64 6F 62 65 " x:xmptk="Adobe
00 00 00 B0 20 58 4D 50 20 43 6F 72 65 20 34 2E 31 2D 63 30 XMP Core 4.1-c0
00 00 00 C0 33 36 20 34 36 2E 32 37 36 37 32 30 2C 20 4D 6F 36 46.276720, Mo
00 00 00 D0 6E 20 46 65 62 20 31 39 20 32 30 30 37 20 32 32 n Feb 19 2007 22
00 00 00 E0 3A 31 33 3A 34 33 20 20 20 20 20 20 22 3E :13:43 ">
00 00 00 F0 0A 20 3C 72 64 66 3A 52 44 46 20 78 6D 6C 6E 73 . <rdf:RDF xmlns:
00 00 01 00 3A 72 64 66 3D 22 68 74 74 70 3A 2F 2F 77 77 77 :rdf="http://www
00 00 01 10 2E 77 33 2E 6F 72 67 2F 31 39 39 39 2F 30 32 2F .w3.org/1999/02/
00 00 01 20 32 32 2D 72 64 66 2D 73 79 6E 74 61 78 2D 6E 73 22-rdf-syntax-ns
00 00 01 30 23 22 3E 0A 20 20 3C 72 64 66 3A 44 65 73 63 72 #">. <rdf:Descri
00 00 01 40 69 70 74 69 6F 6E 20 72 64 66 3A 61 62 6F 75 74 ption rdf:about
```