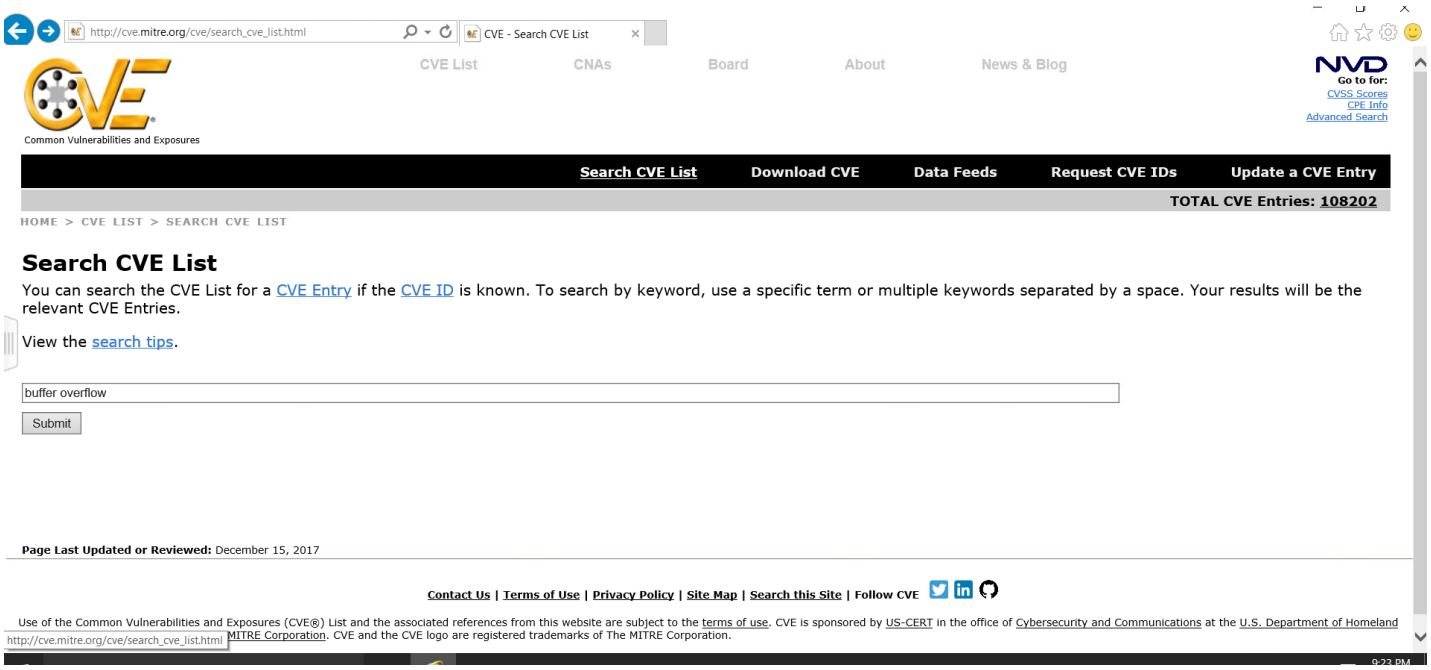
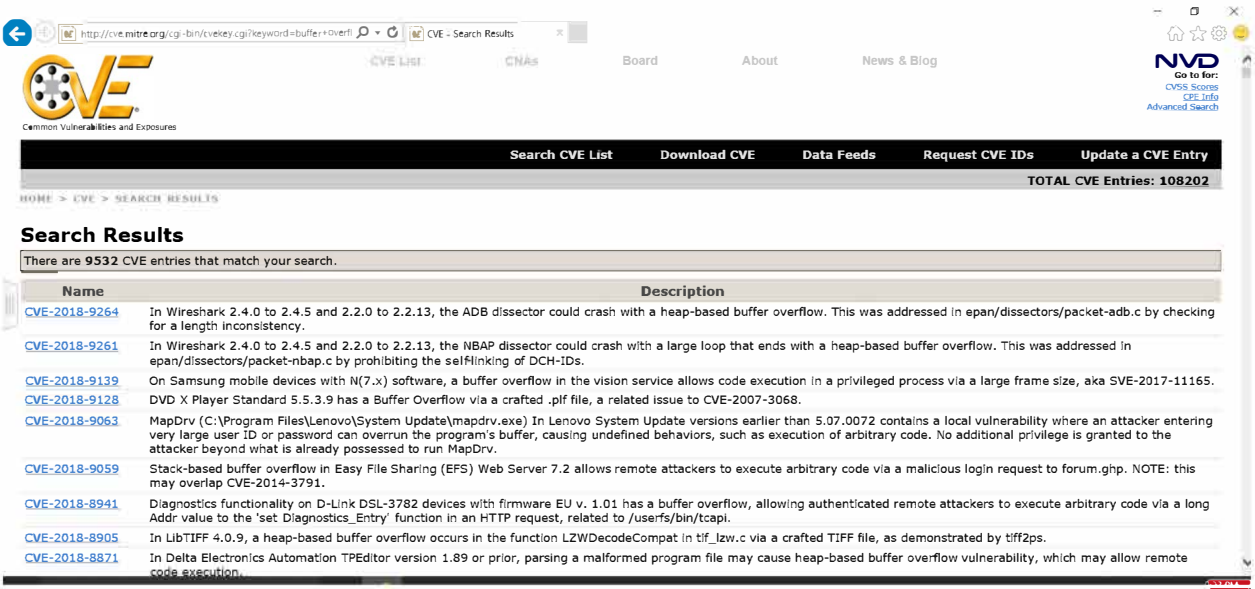
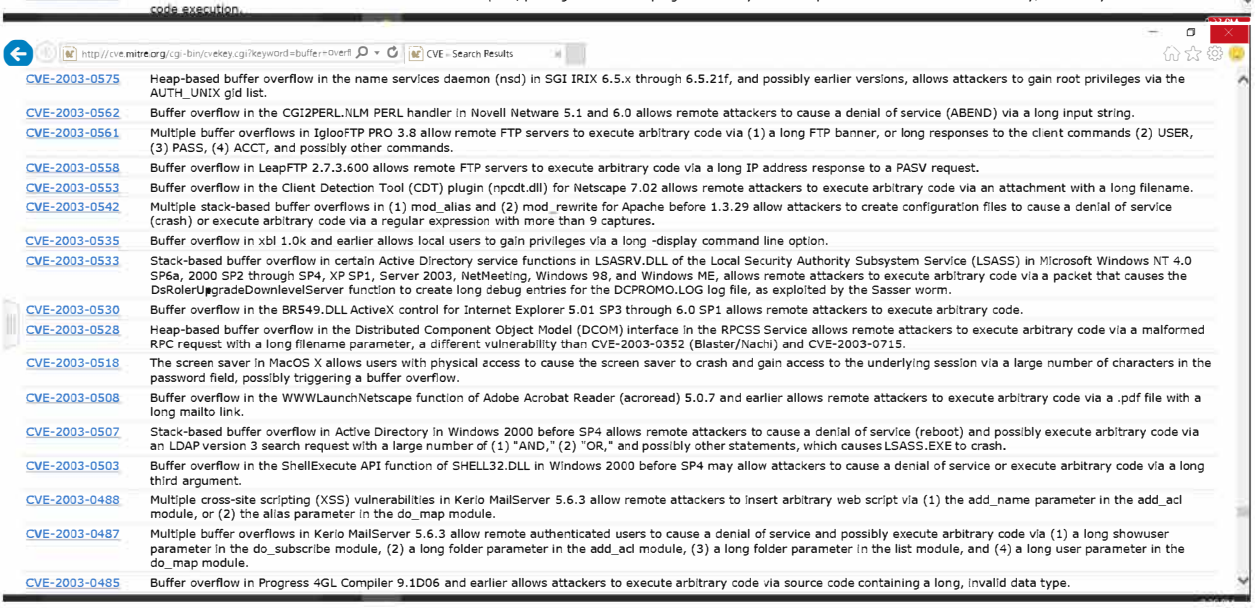
7.1 Review CVEs and Buffer Overflows

Enter buffer overlow in keyword search

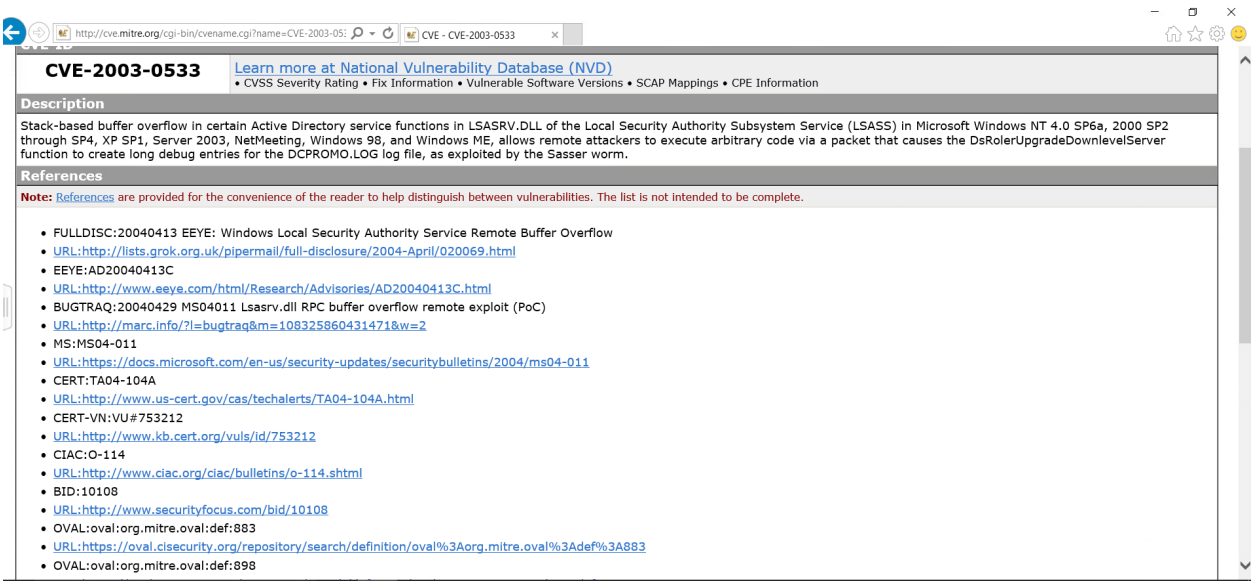


Search Results

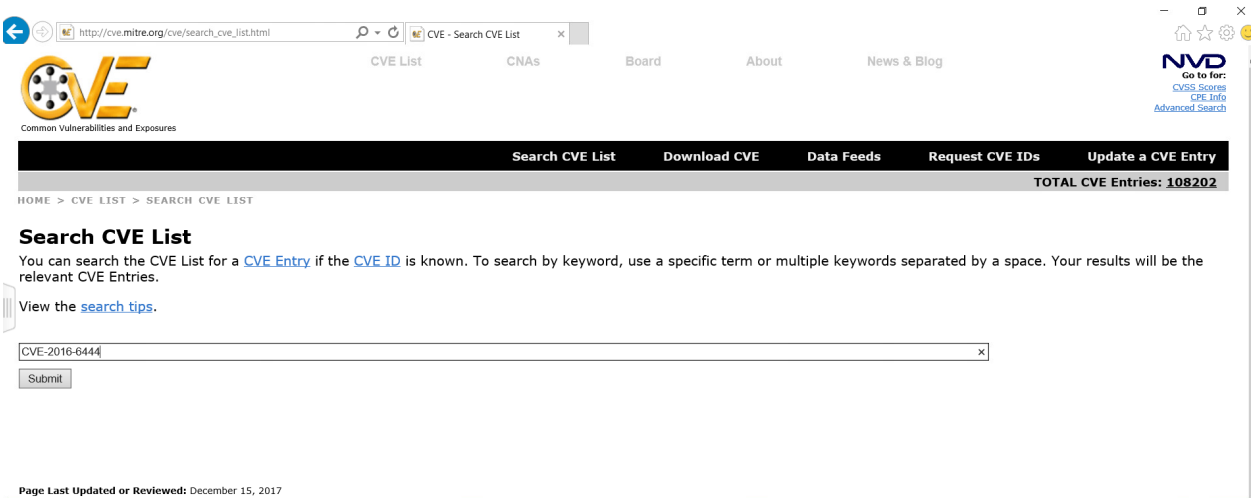

http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=buffer+overfl
CVE - Search Results
CVE List
CNAs
Board
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search
Common Vulnerabilities and Exposures
Search CVE List
Download CVE
Data Feeds
Request CVE IDs
Update a CVE Entry
TOTAL CVE Entries: 108202
HOME > CVE > SEARCH RESULTS
Search Results
There are 9532 CVE entries that match your search.
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 2.4.0 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 self-linking 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 /userfs/bin/tcapi.
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.


http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=buffer+overfl
CVE - Search Results
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 (npcdt.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 xbl 1.0x 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 DCPROMO.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 filename parameter, a different vulnerability than CVE-2003-0352 (Blaster/Nachi) and CVE-2003-0715.
CVE-2003-0518
The screen saver in MacOS 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.

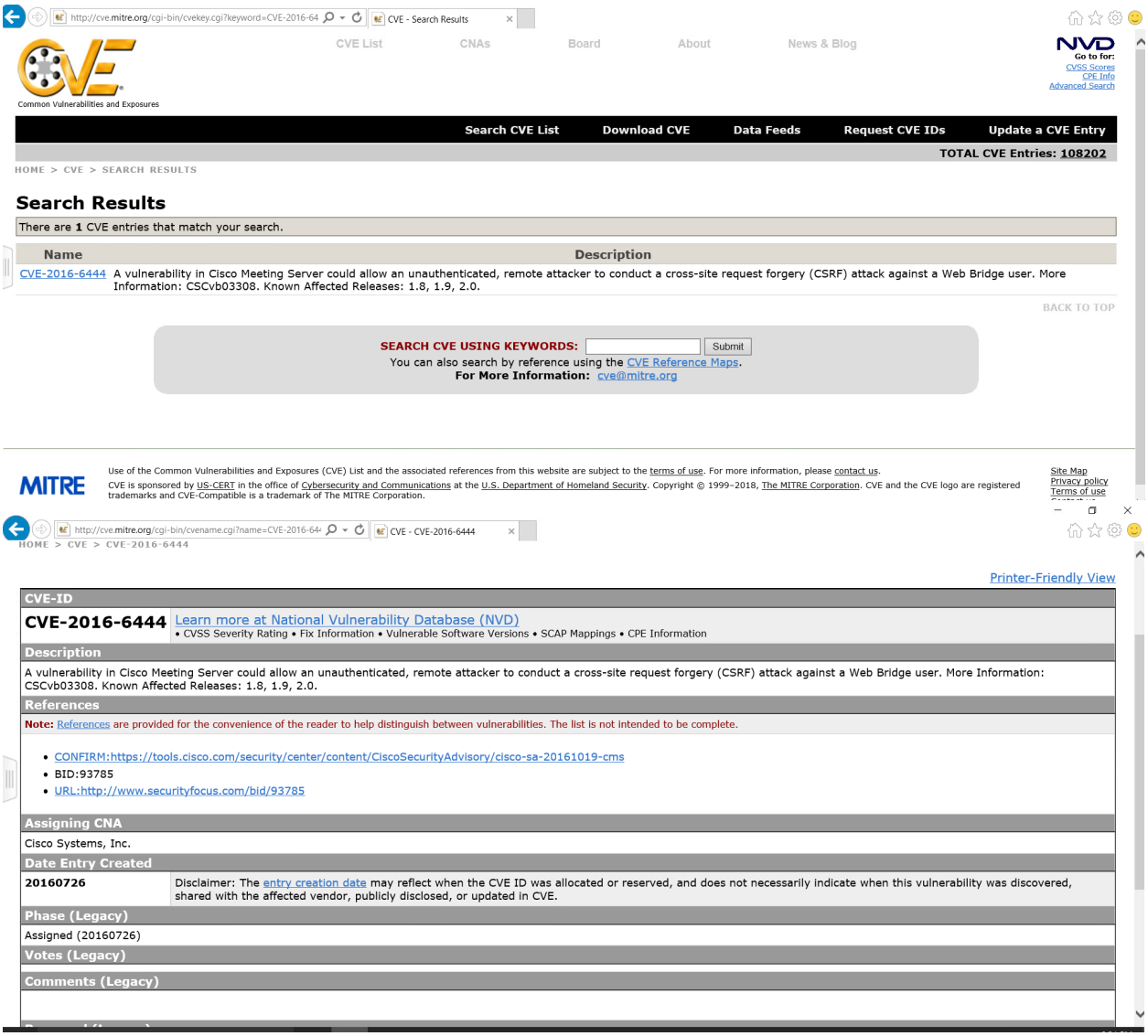
The worm the exploited CVE-2003-0553 is the Sasser Worm.



Search for CVE-2016-6444



CSRF



http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2016-64 CVE - Search Results

CVE List CNAs Board About News & Blog

Common Vulnerabilities and Exposures

NVD Go to for: CVSS Scores CPE Info Advanced Search

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

TOTAL CVE Entries: 108202

HOME > CVE > SEARCH RESULTS

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.

BACK TO TOP

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

MITRE

Use of the Common Vulnerabilities and Exposures (CVE) List and the associated references from this website are subject to the terms of use. For more information, please contact us.

CVE is sponsored by US-CERT in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Copyright © 1999–2018, The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compatible is a trademark of The MITRE Corporation.

Site Map Privacy policy Terms of use

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-64 CVE - CVE-2016-6444

HOME > CVE > CVE-2016-6444

Printer-Friendly View

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)

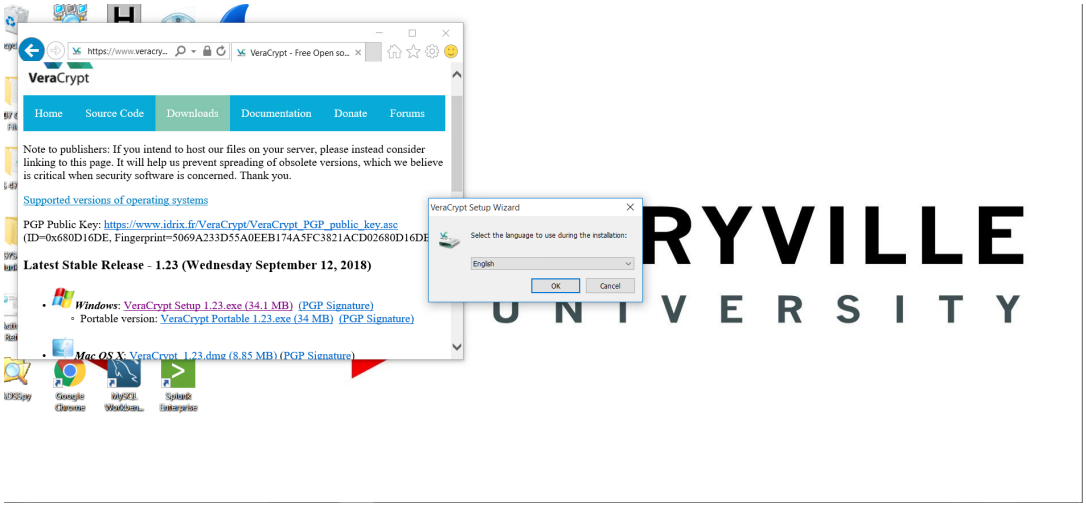
Assigned (20160726)

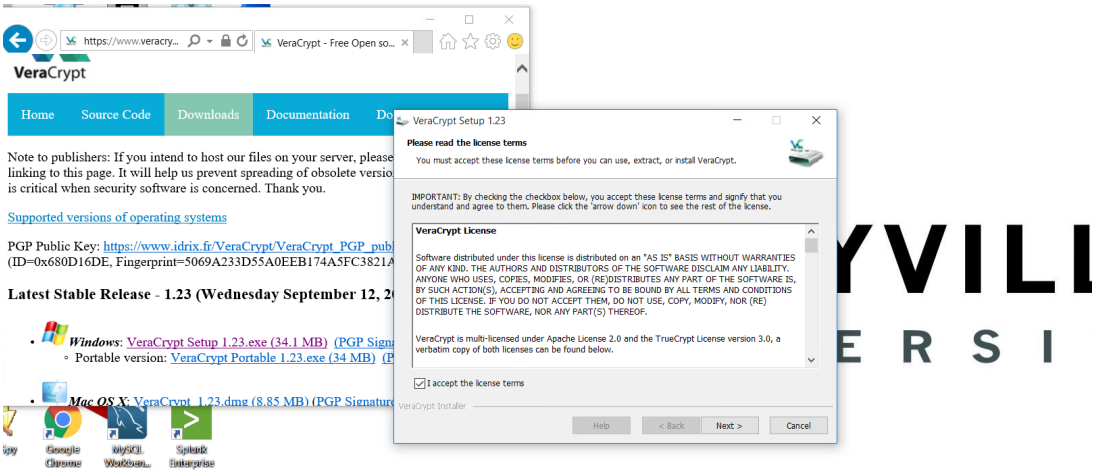
Votes (Legacy)

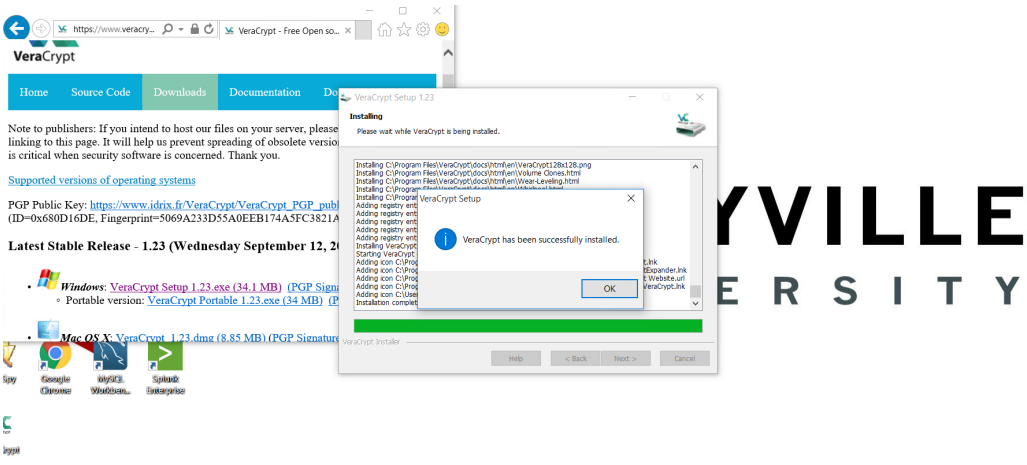
Comments (Legacy)

10.1 Encrypting Data at Rest for Added Physical Security

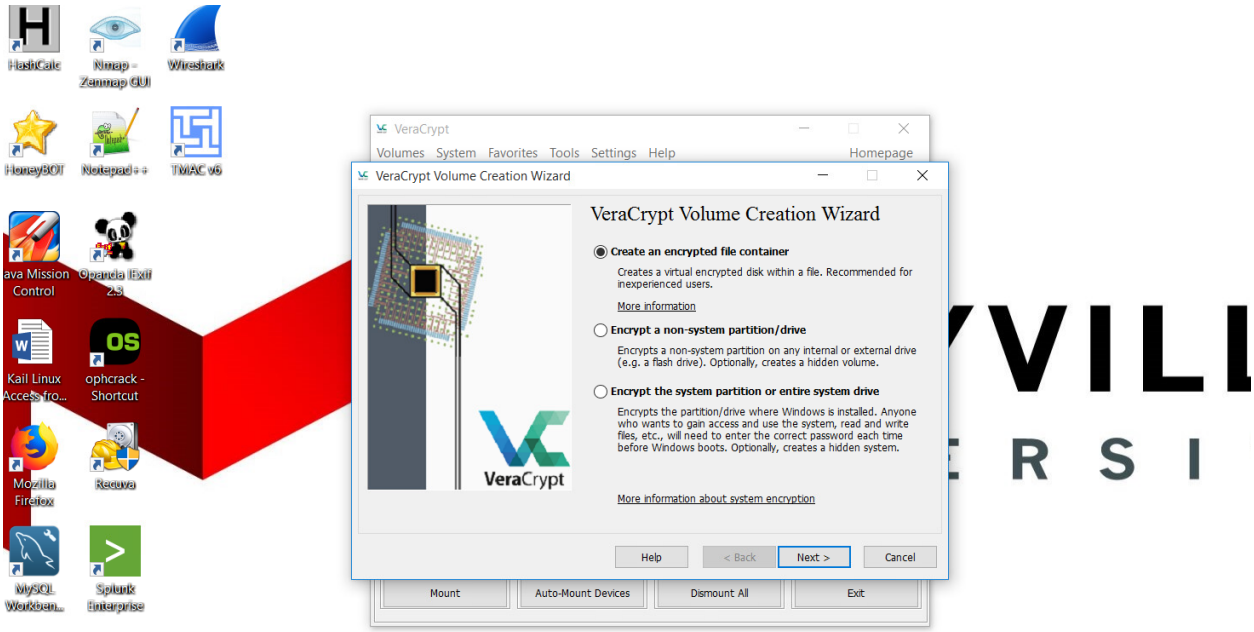
Download and install VeraCrypt

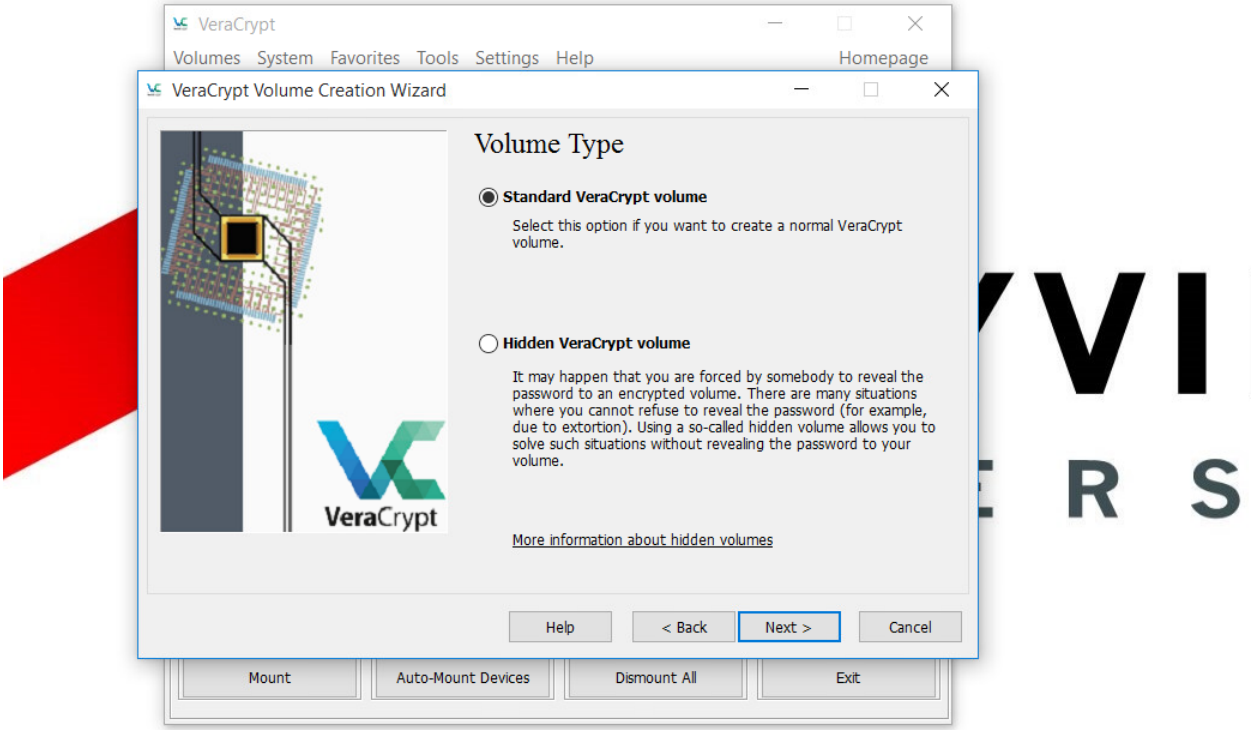




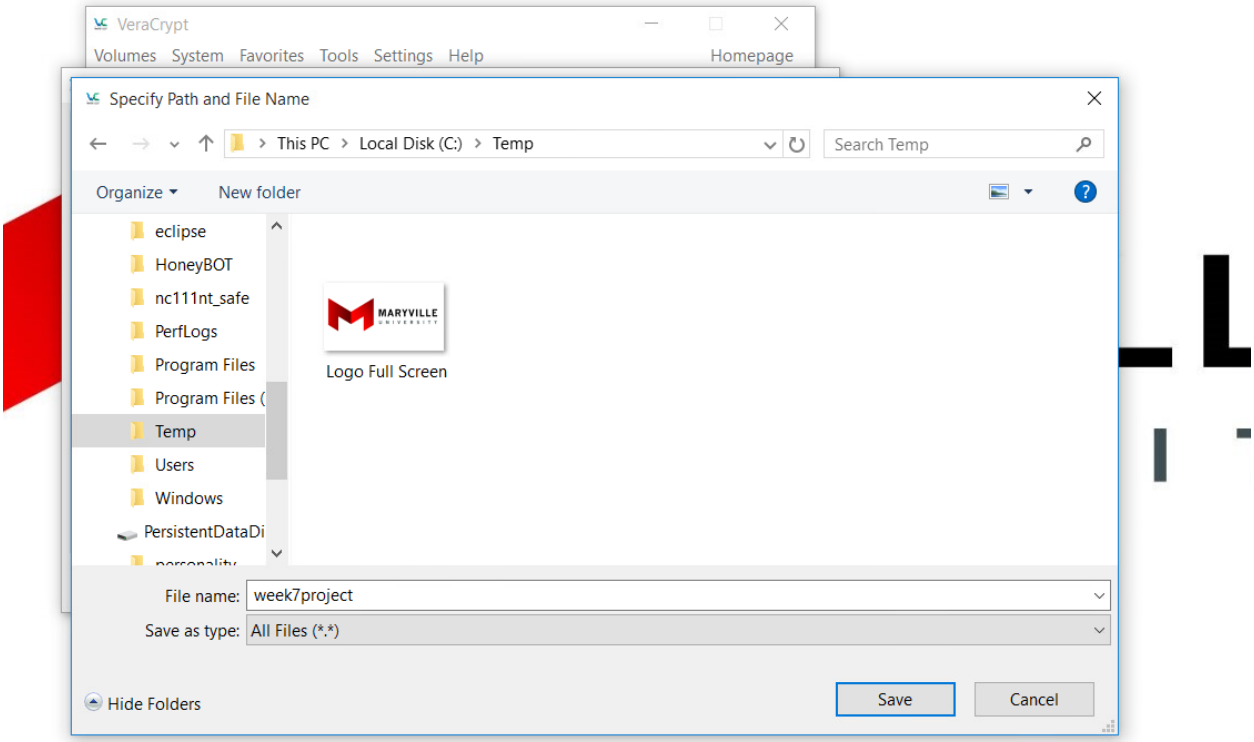


Create Volume

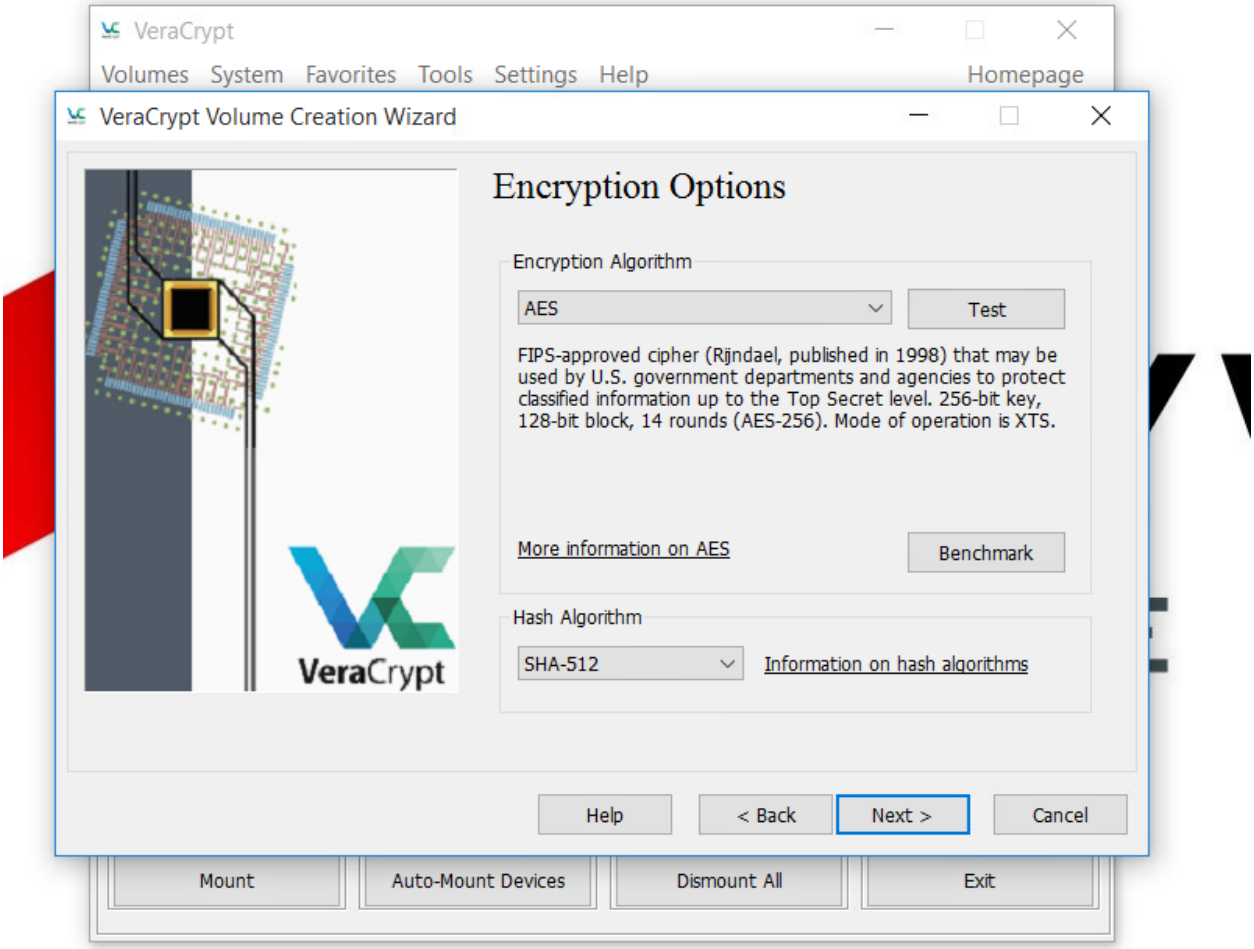




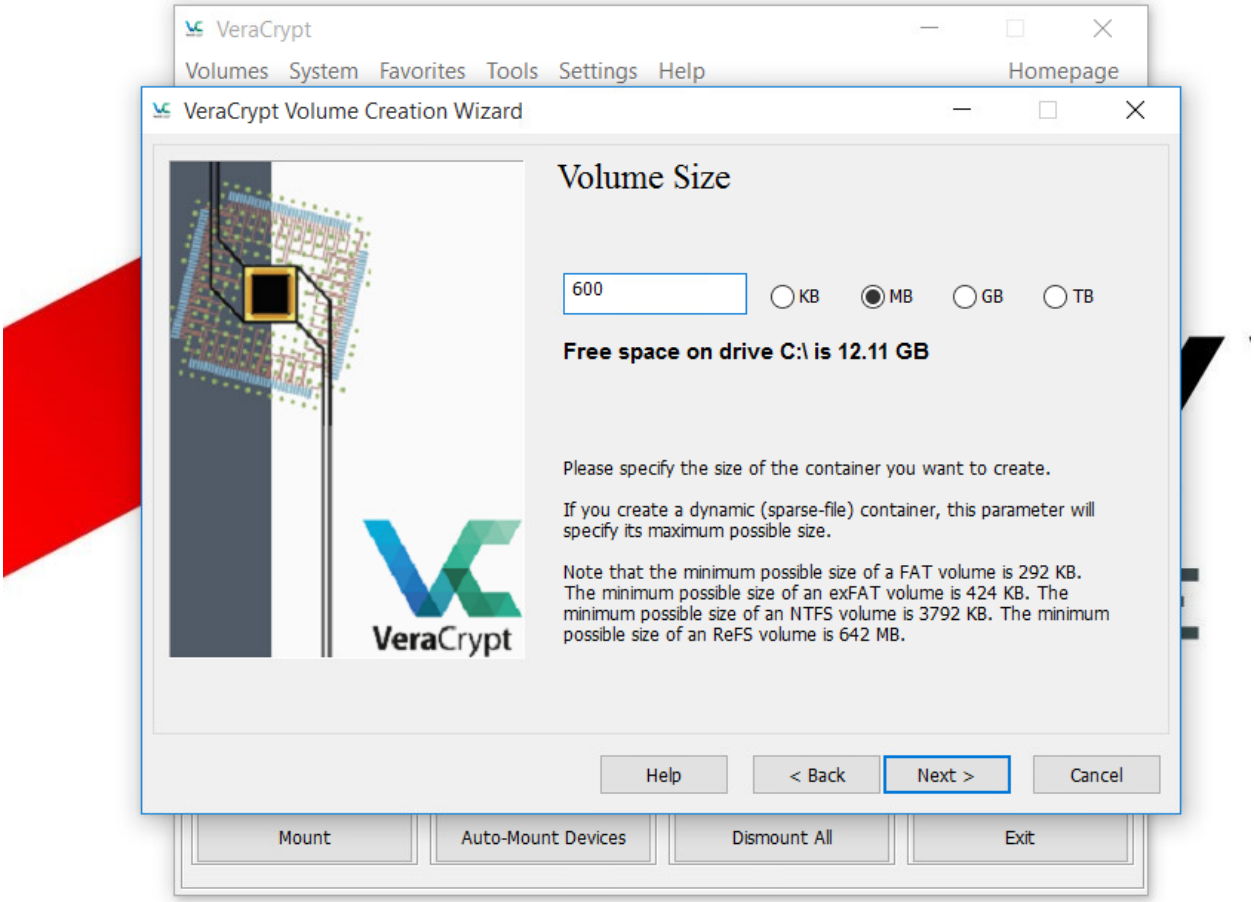
Choose location and Name file



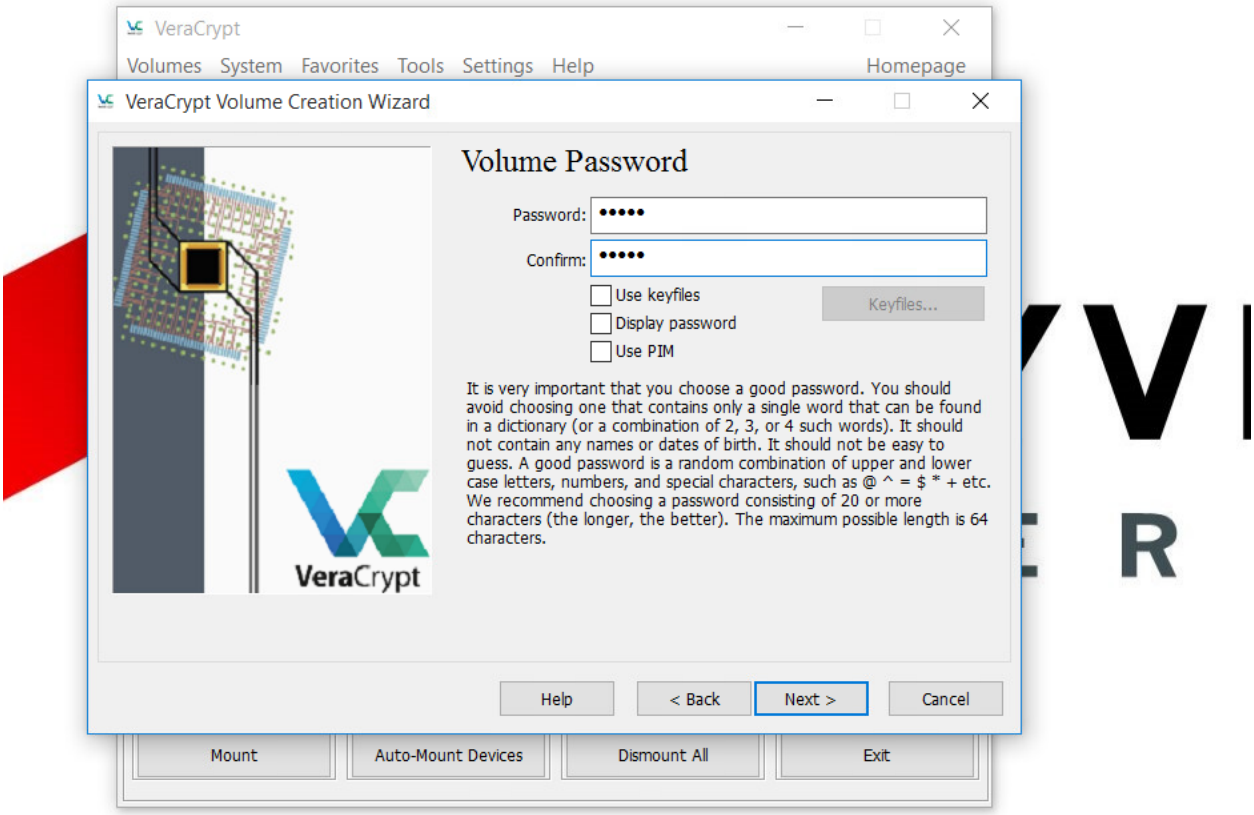
Default setting for encryption alogrithm and hash logarithm for volume



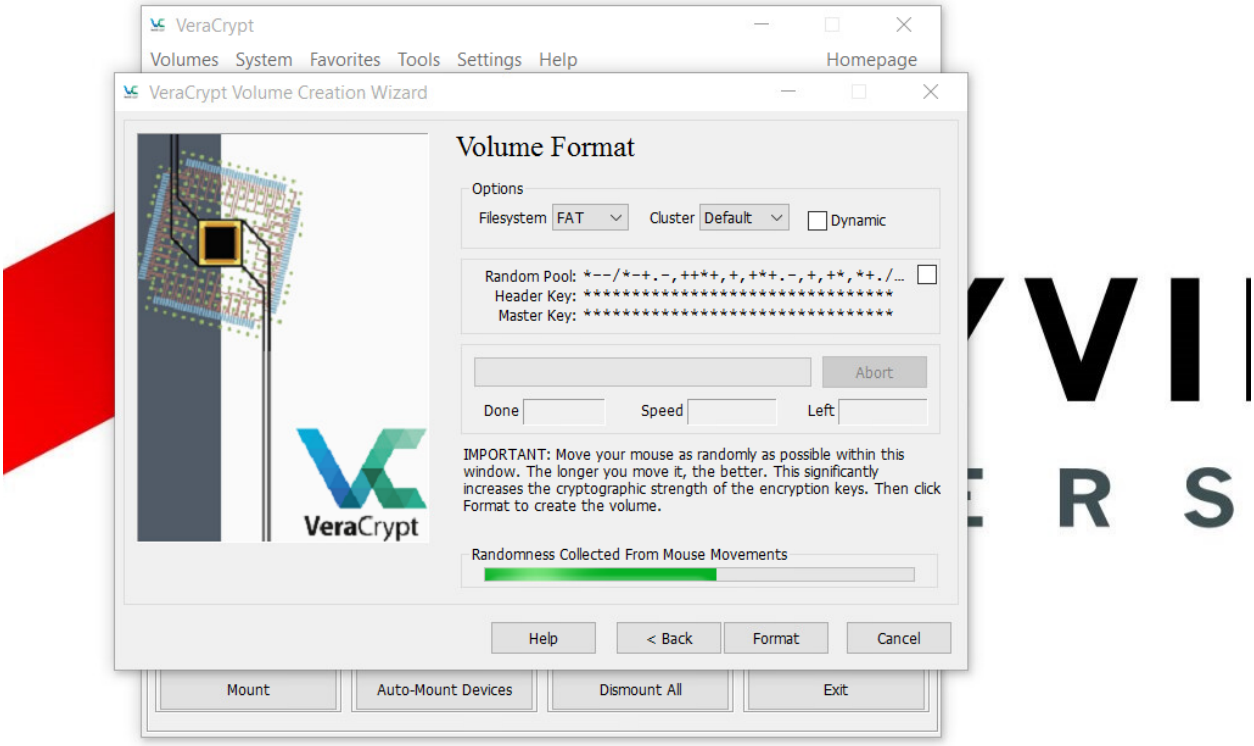
Specify size of VeraCrypt container



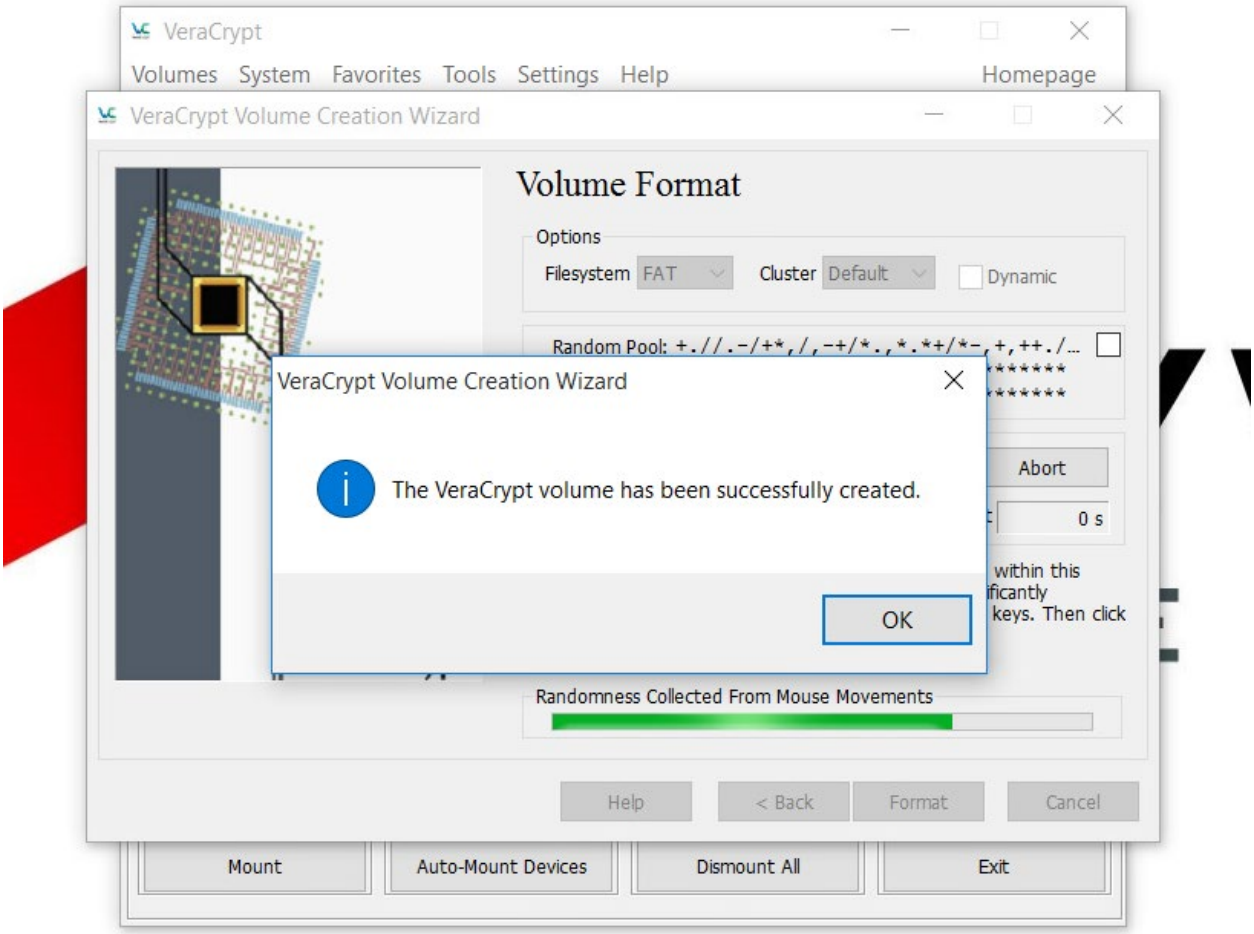
Create volume password

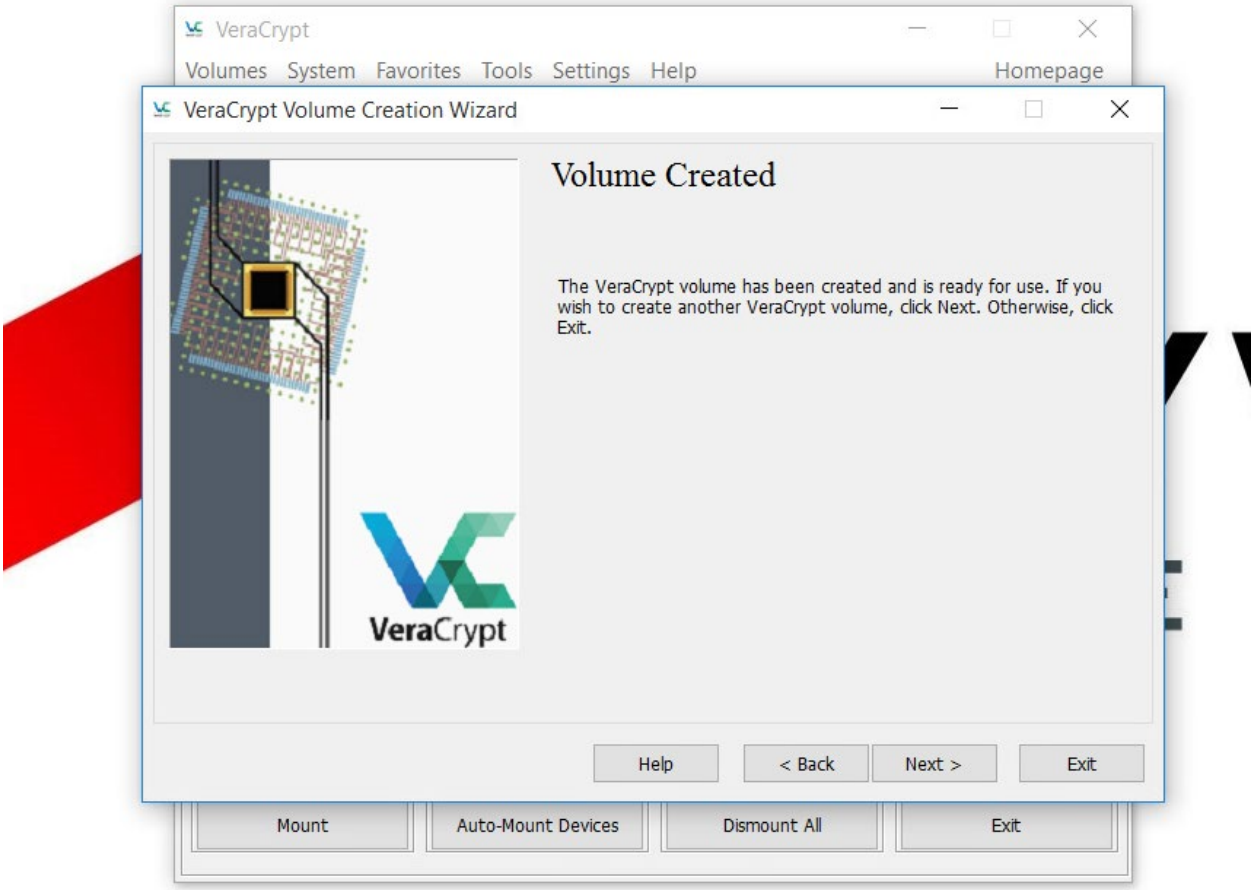


Move mouse around so that randomness indicator becomes green



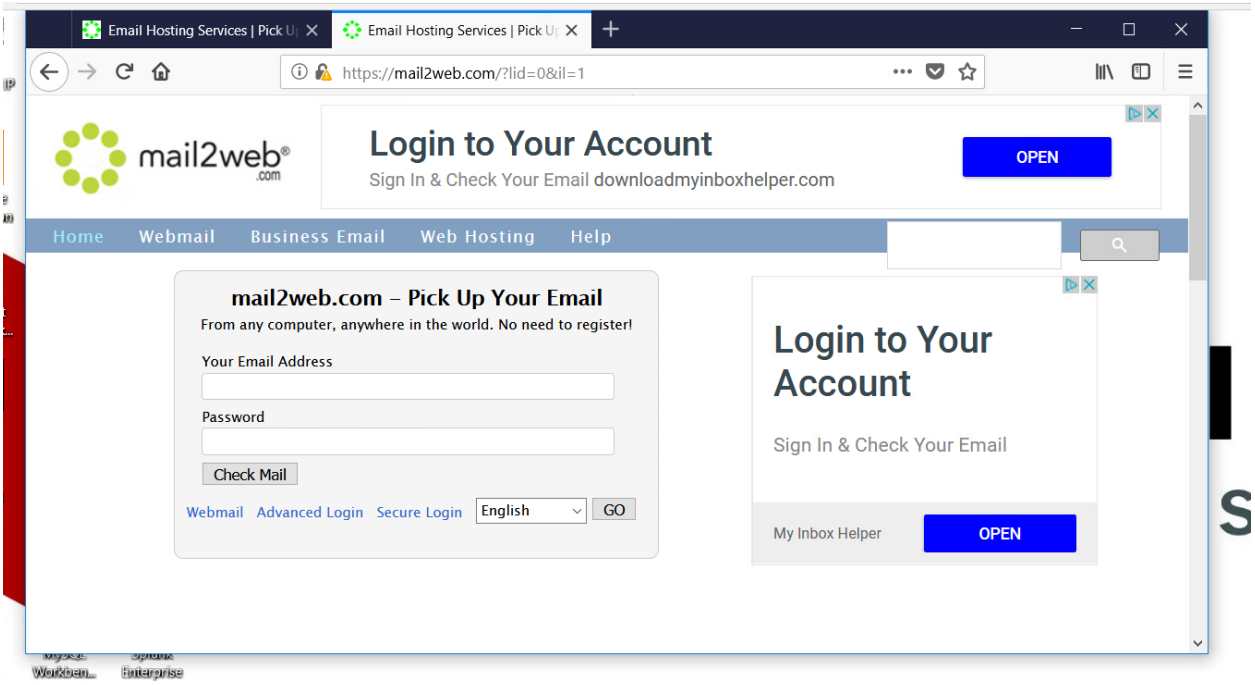
Confirmation that VeraCrypt volume has been successfully created.



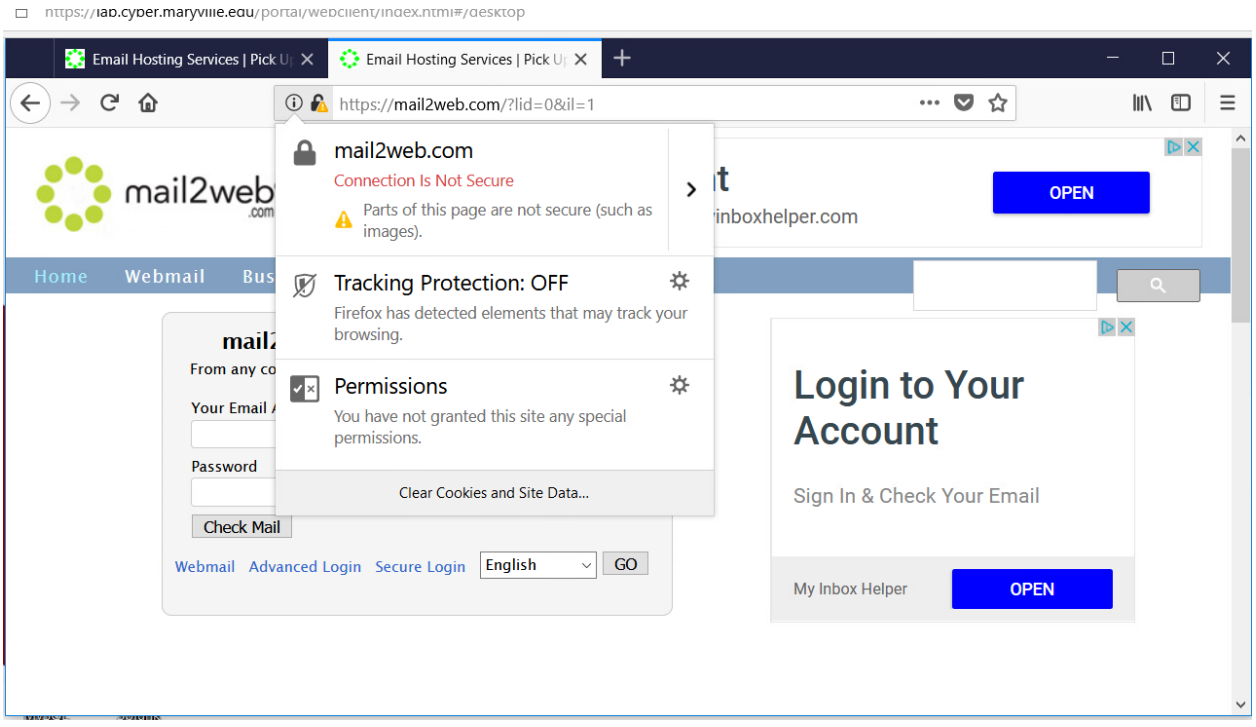

VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
VeraCrypt Volume Creation Wizard
Volume Created
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.
VeraCrypt
Help
< Back
Next >
Exit
Mount
Auto-Mount Devices
Dismount All
Exit

11.1 Examining an SSL Certificate

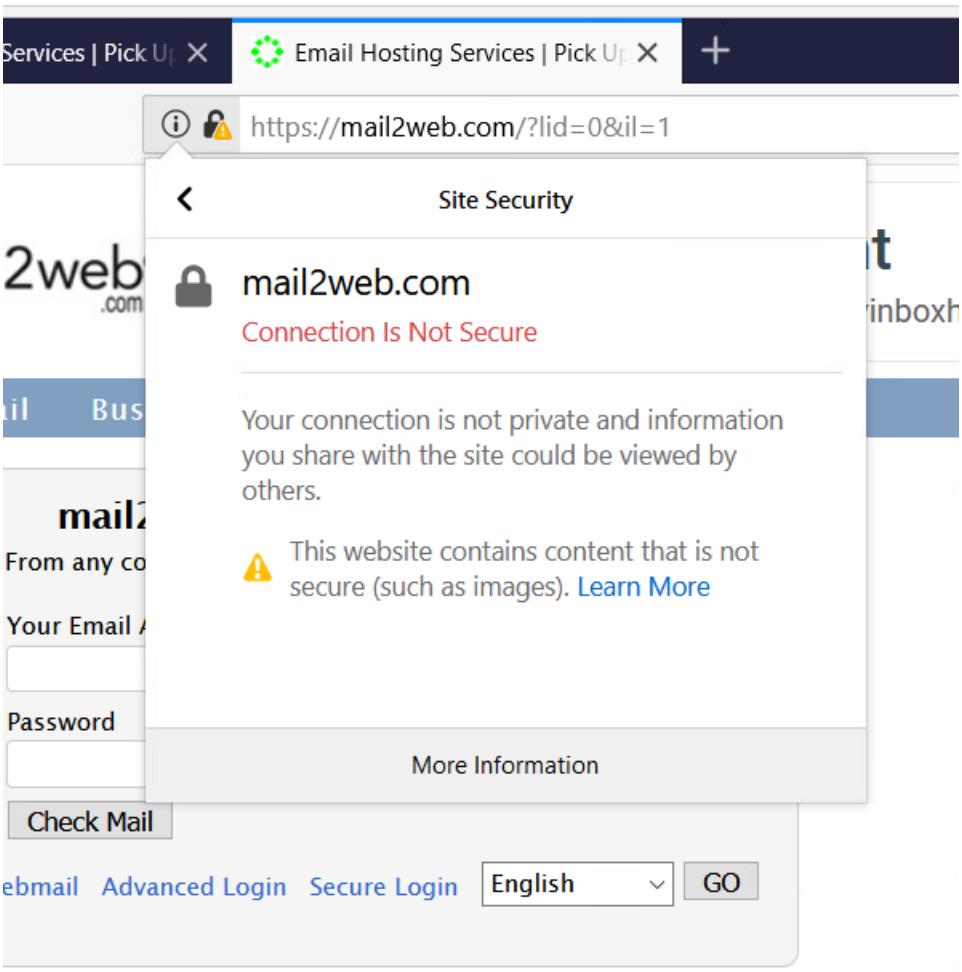
Go to mail2web.com and choose secure login option



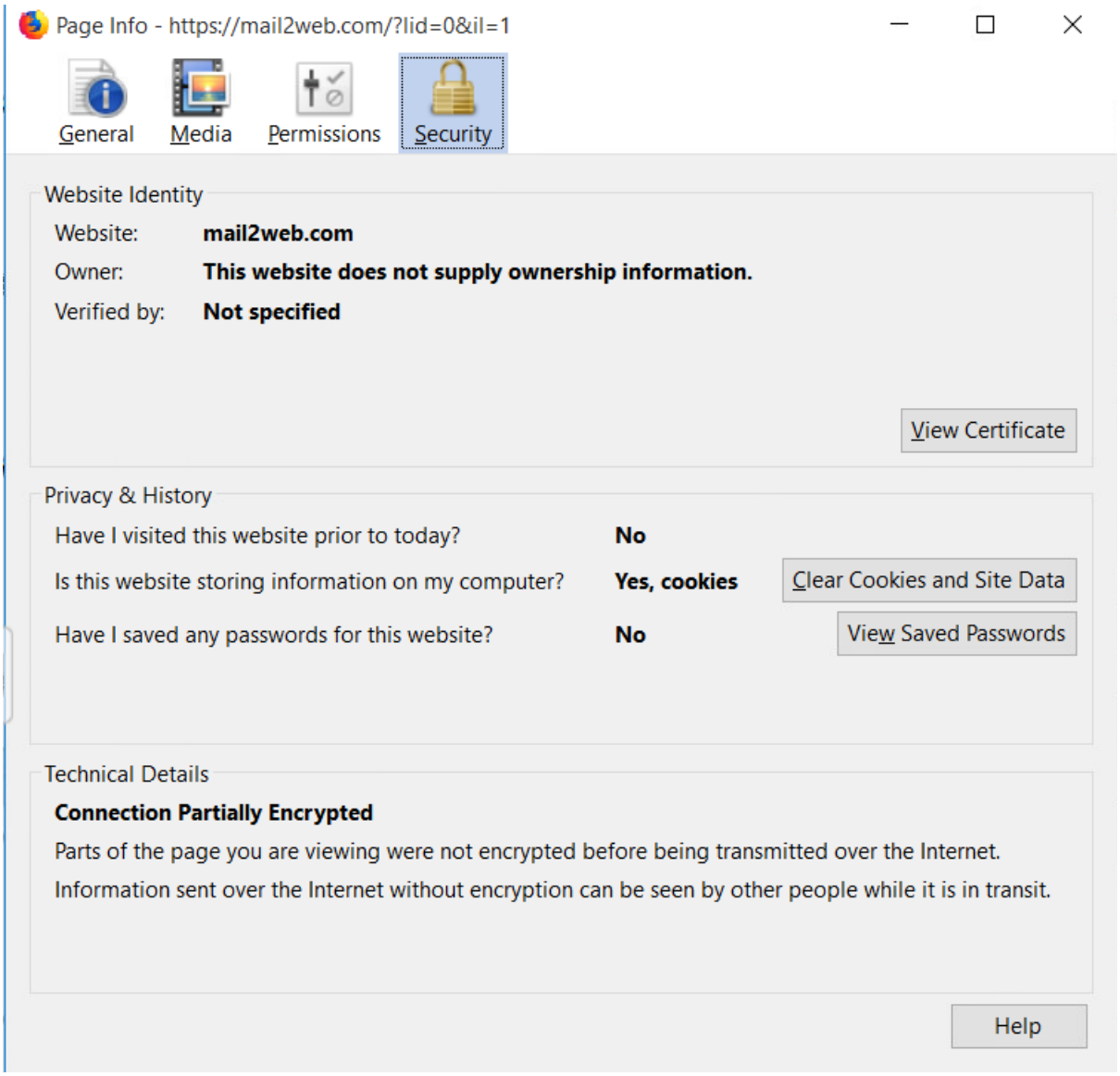
Click SSL icon in the address bar



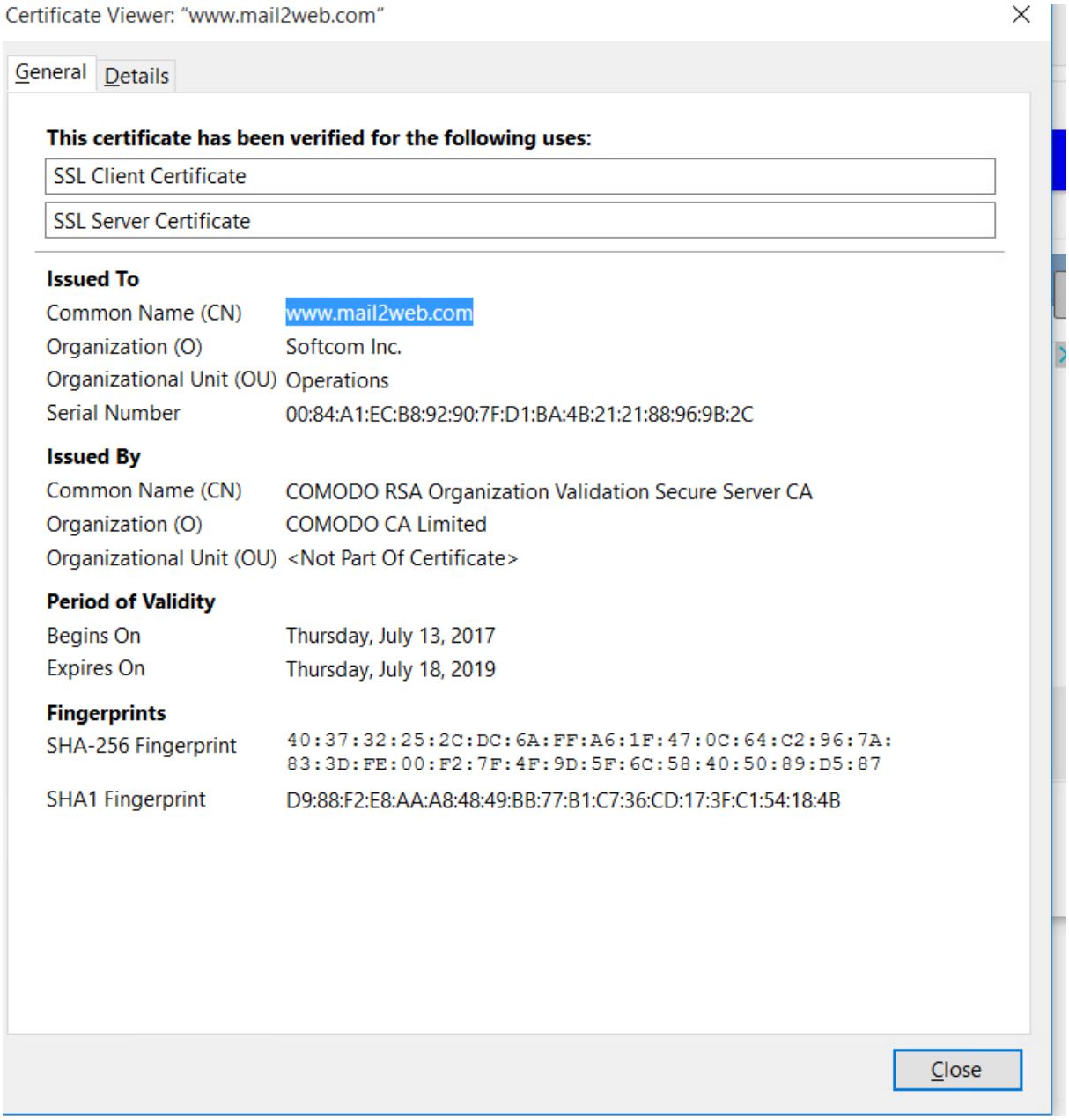
SSL icon information



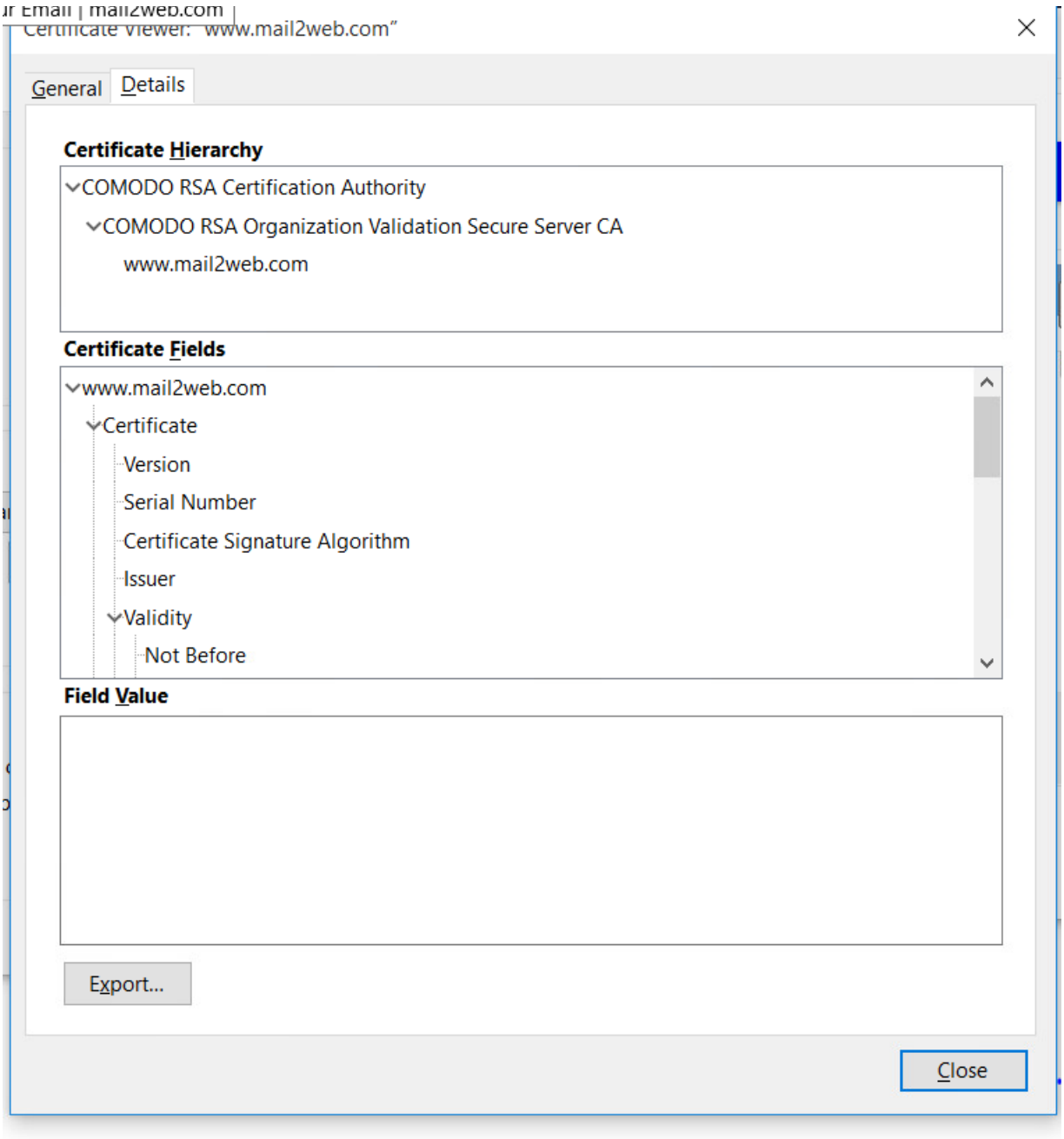
More information from SSL icon in previous pic

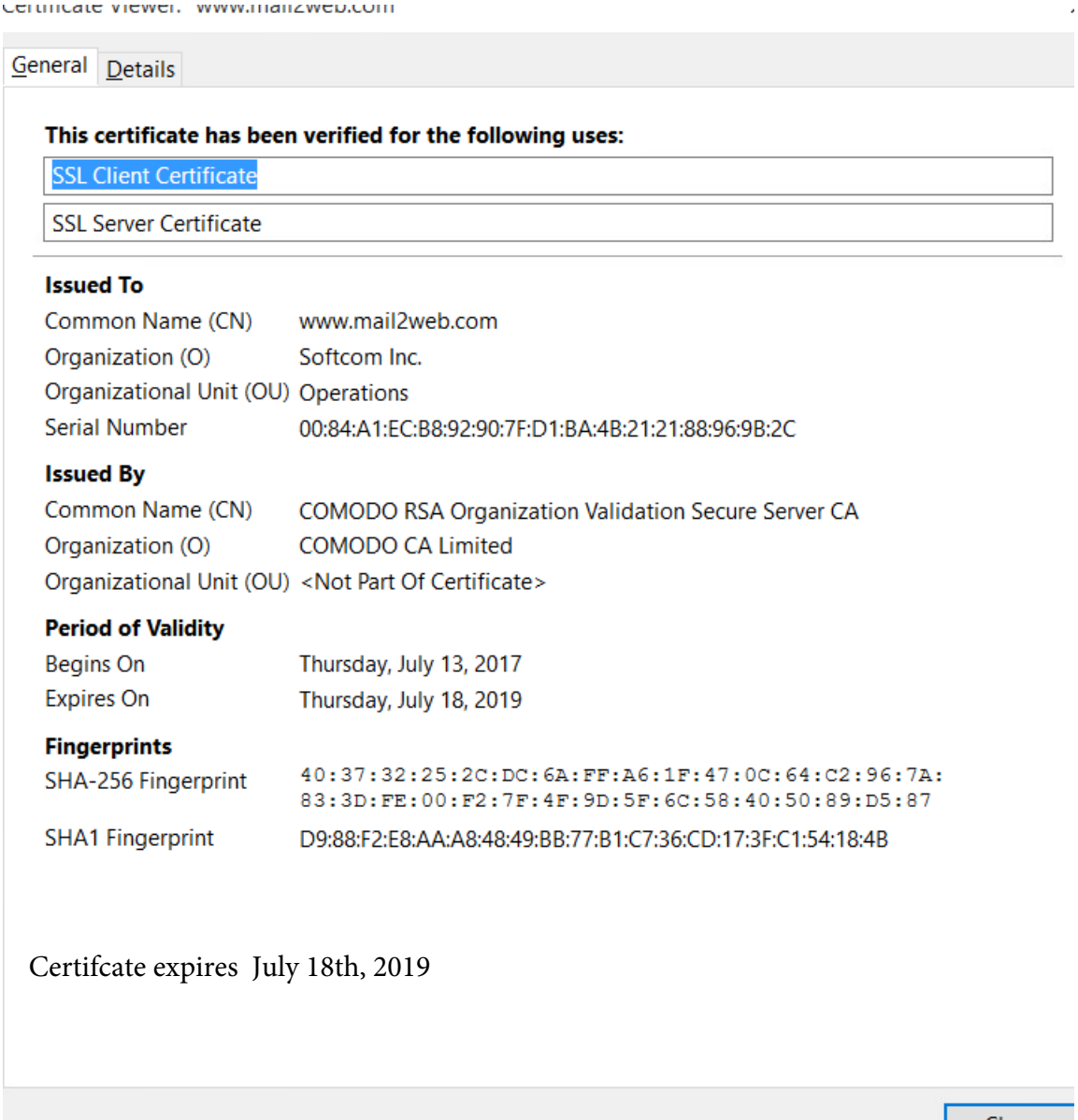


View certificate [general information]

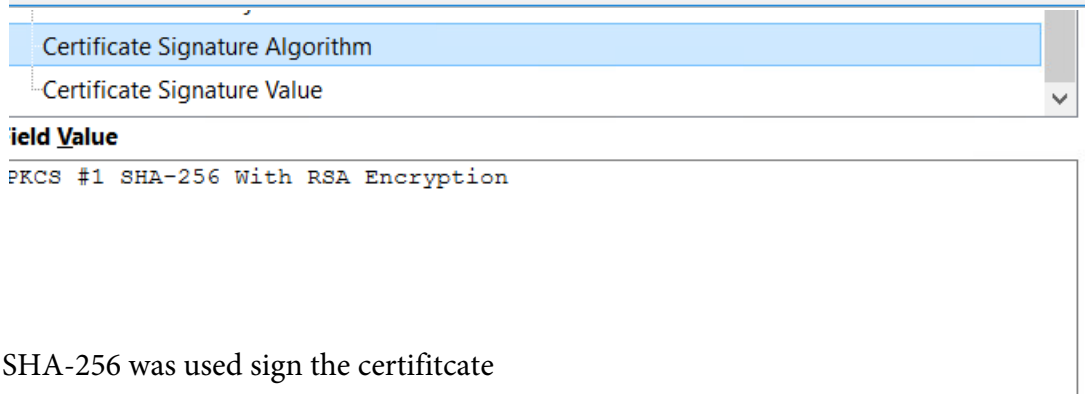


Details of certificate





Certifcate expires July 18th, 2019

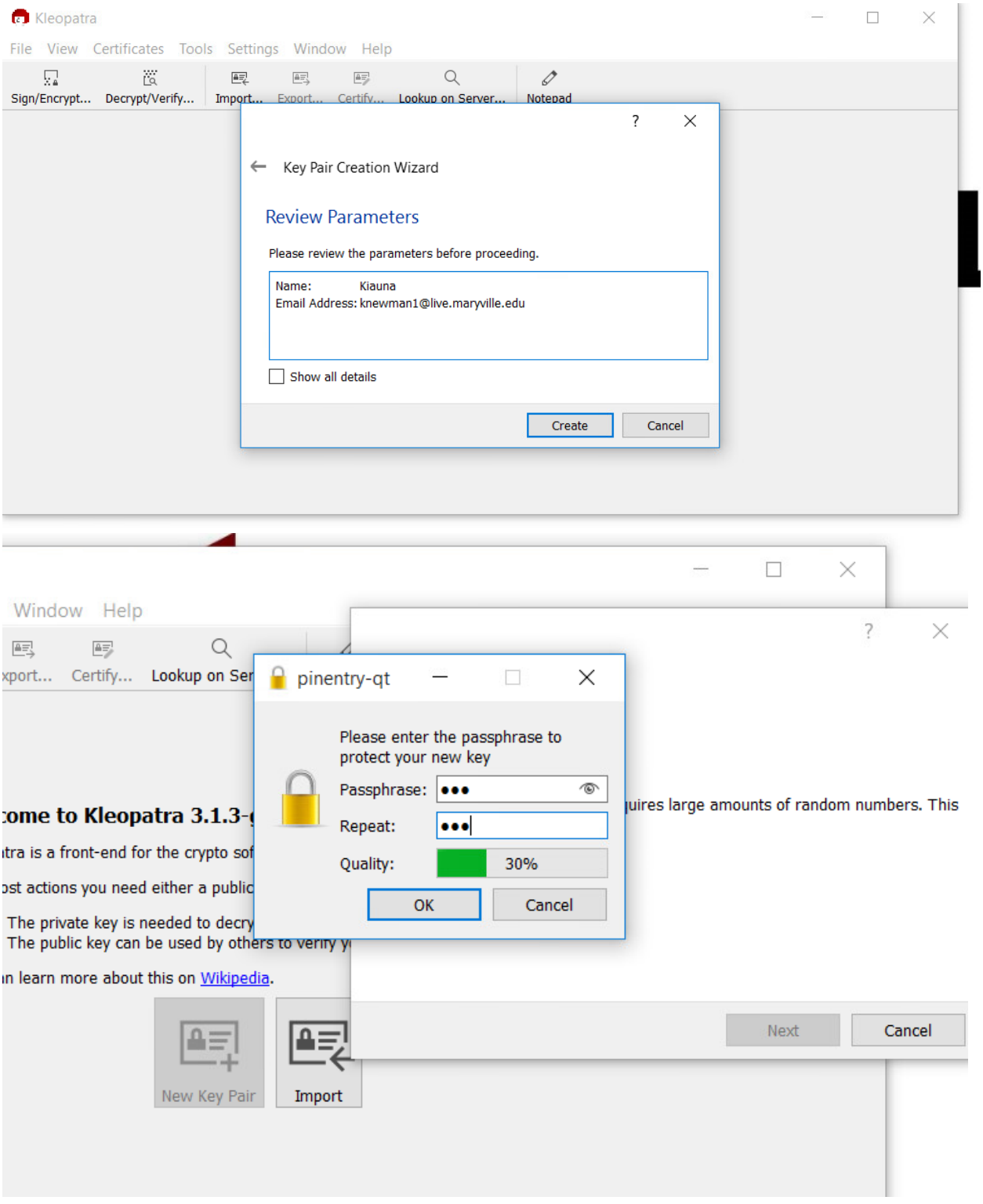


SHA-256 was used sign the certifitcate

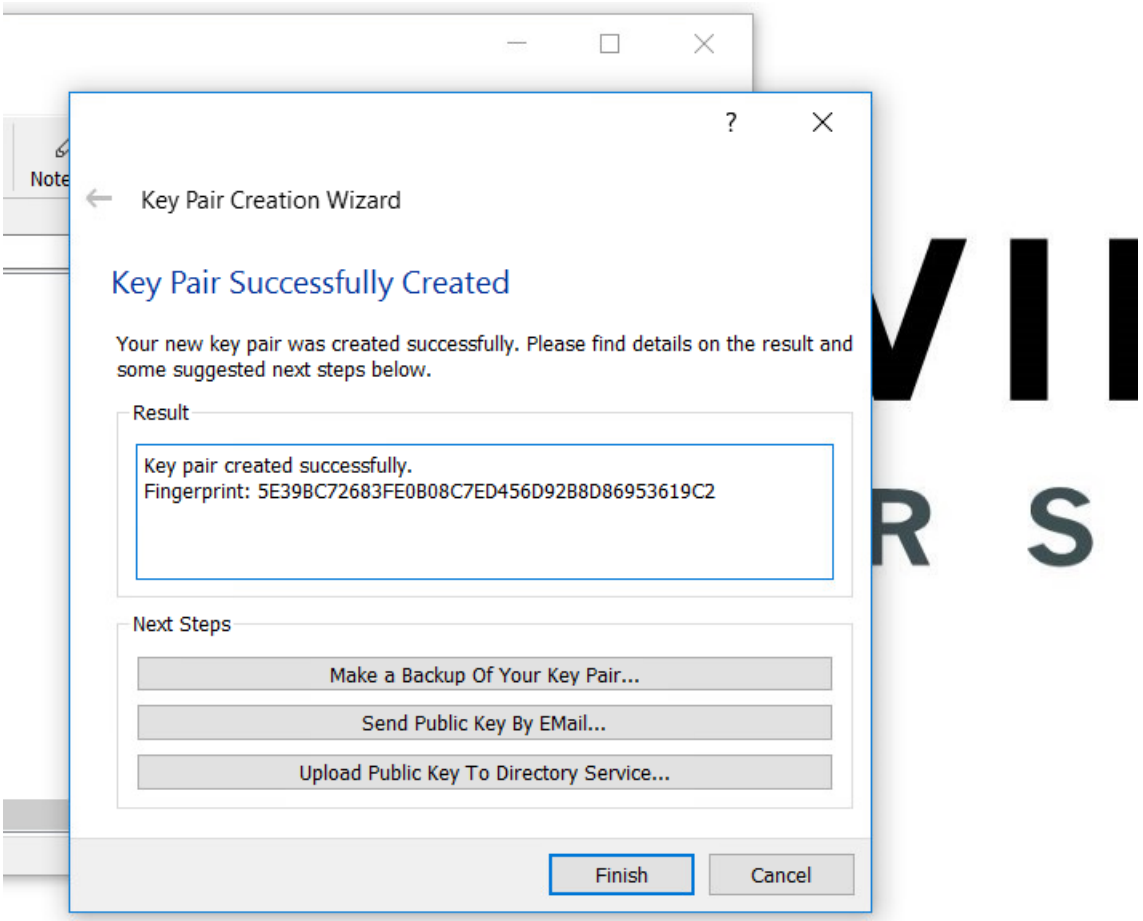
Deliverables

1. Using GPG for Encryption

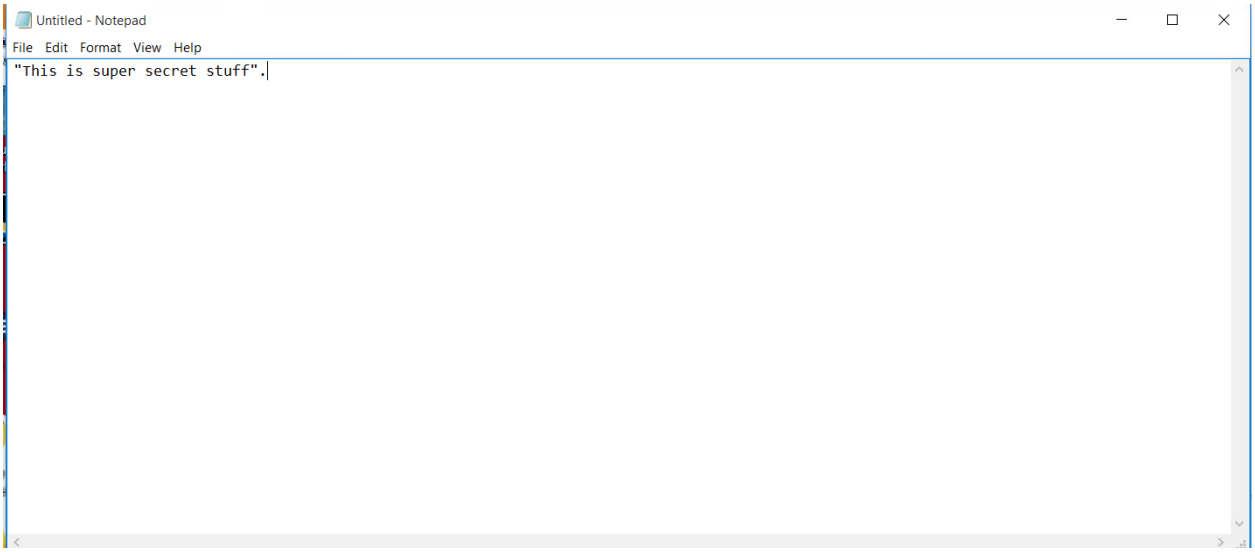
Run Kleopatra to create a New Key Pair.



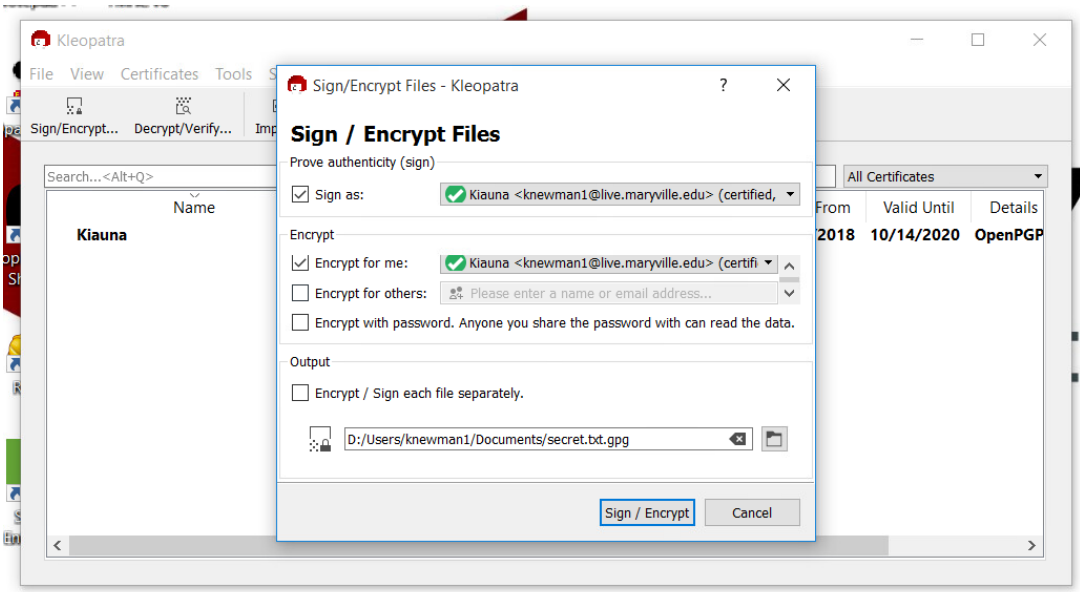
Confirmation that creation of keypair was sucessful



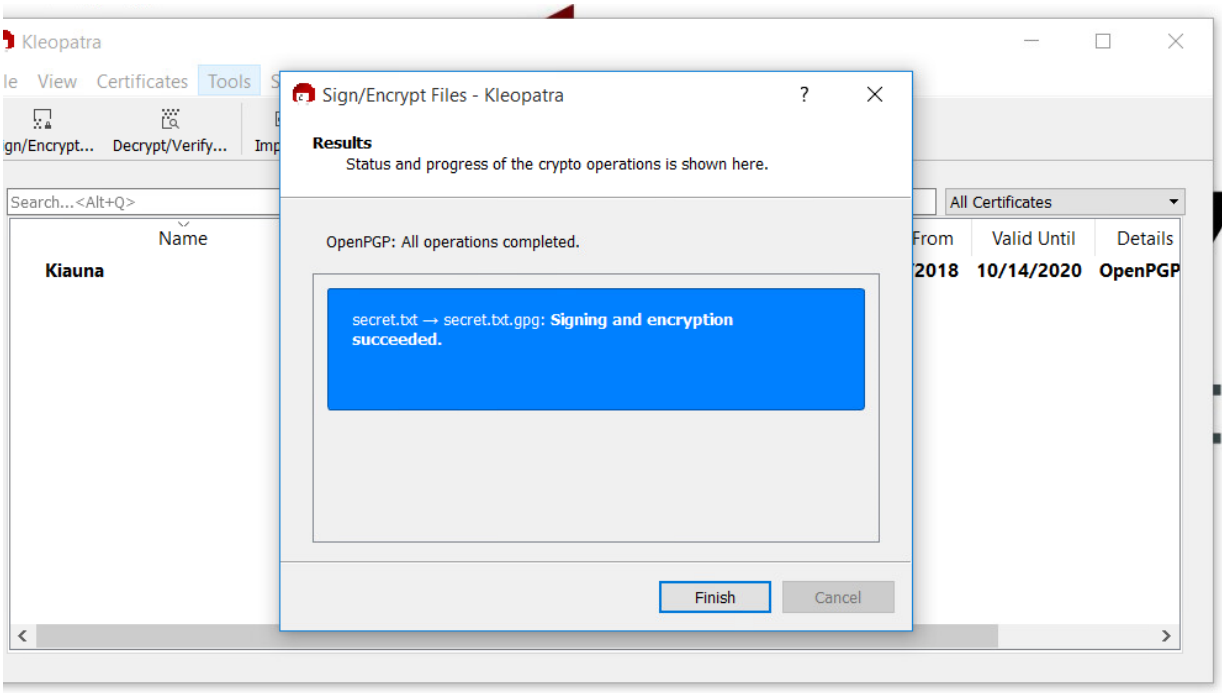
Open Notepad and create a secret.txt file with the text This is super secret stuff inside the file.



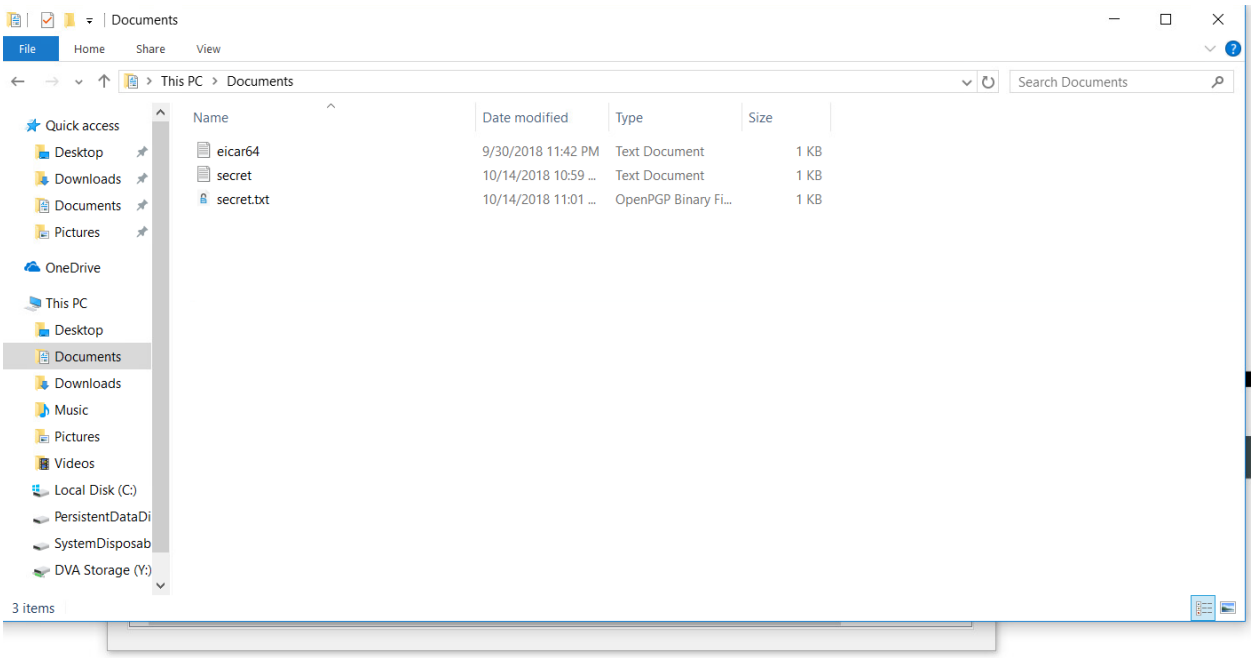
Click on Sign Encrypt in Kleopatra and encrypt the secret.txt file.



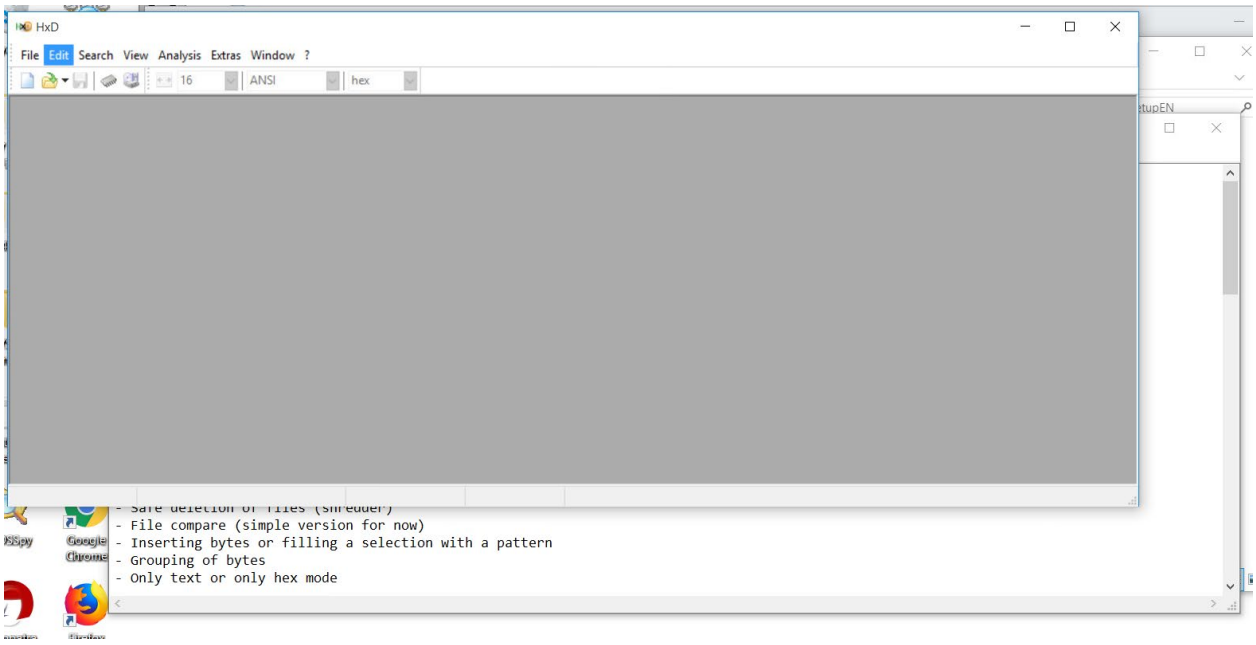
Completion of signing and encryption



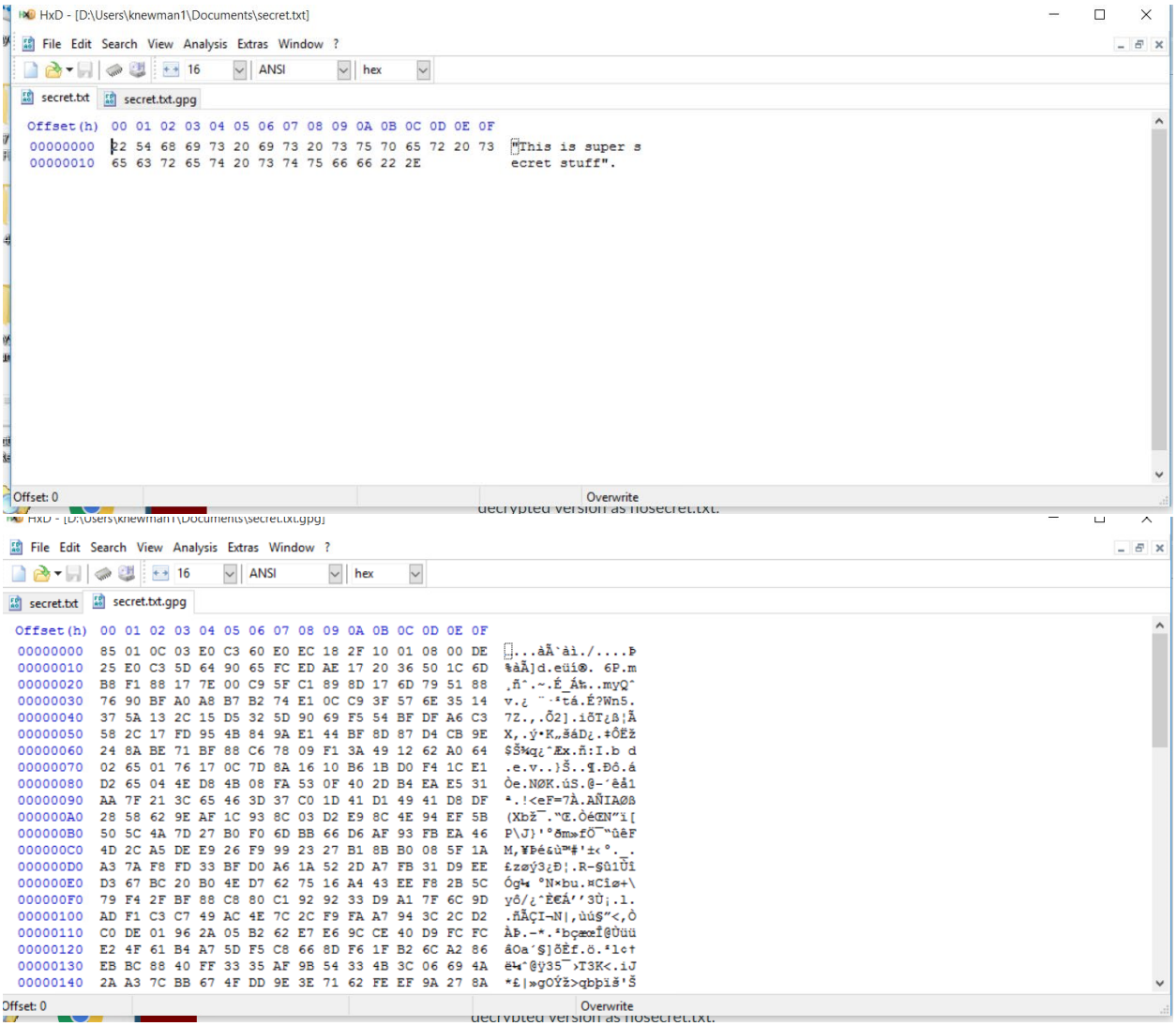
Screen-shot of secret.txt file and secret.txt.gpg file



Opening HxD editor

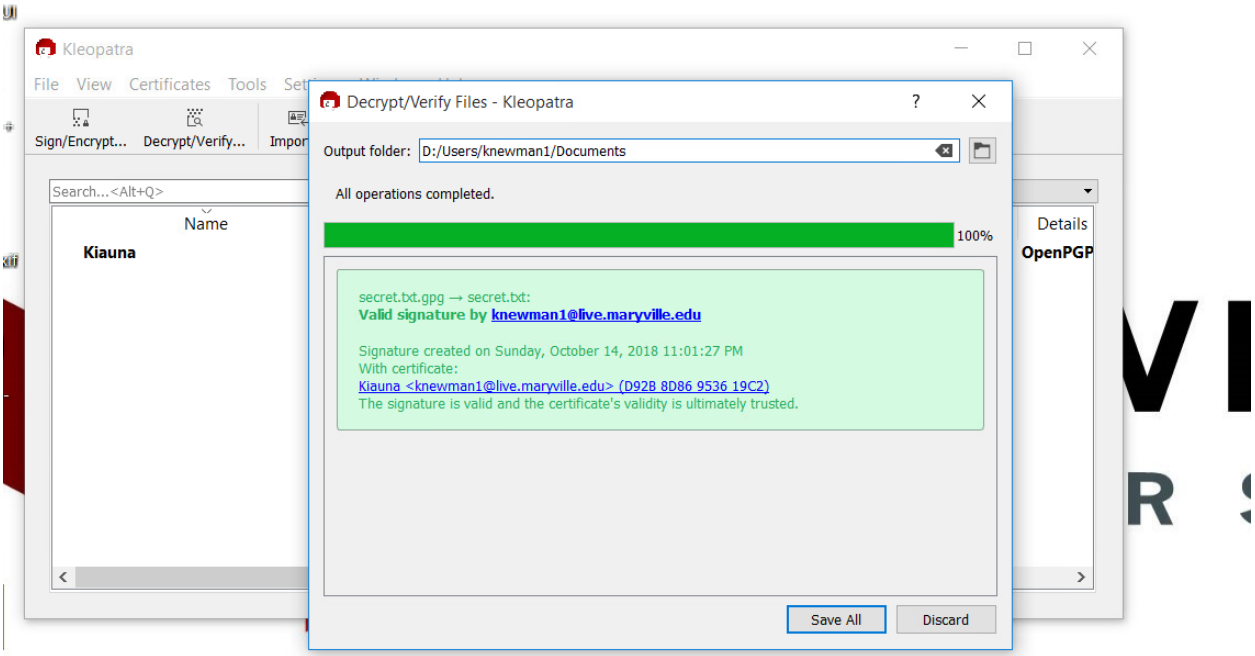


view the secret.txt.gpg file and the secret.txt file.



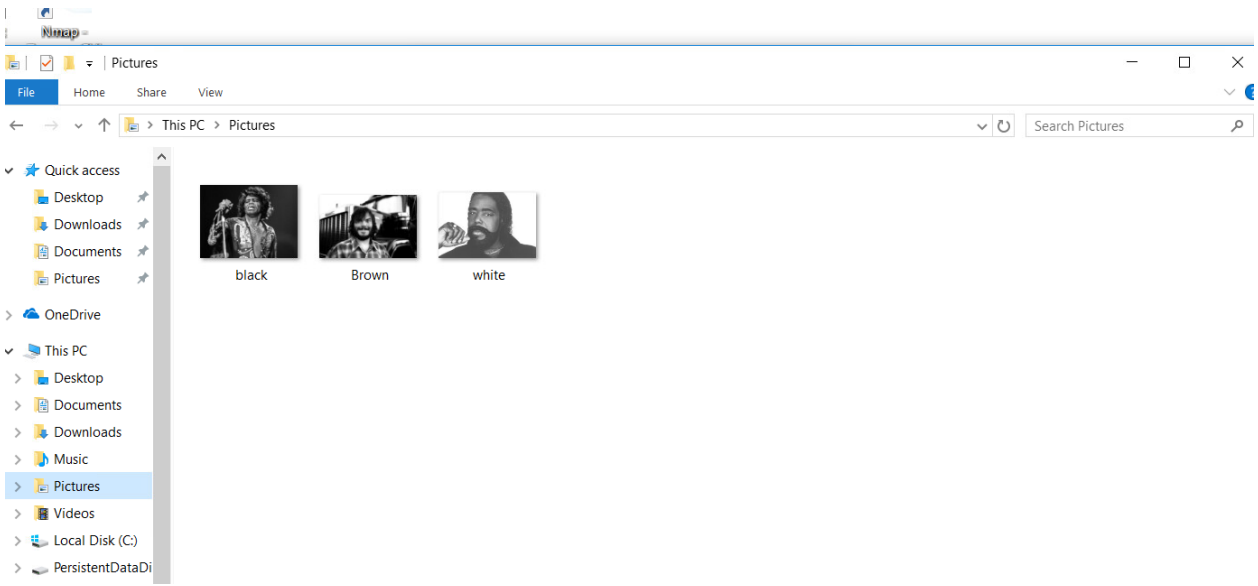
Is there any clear text in the secret.txt.gpg file
There isnt any clear text in the gpg file.
What about the secret.txt file
There phrase this is super secret stuff is shown.
Did you successfully encrypt the file
yes

Decrypt secret.txt.gpg



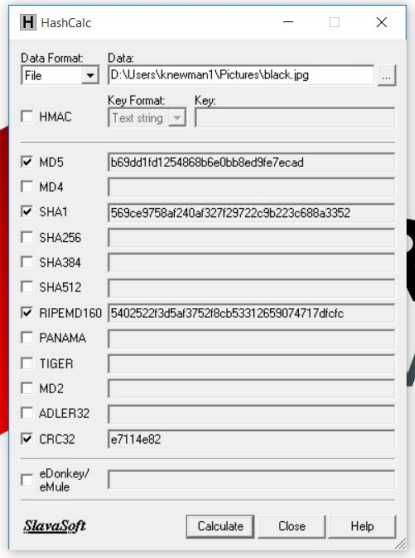
2. MD5 Hash Collisions

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

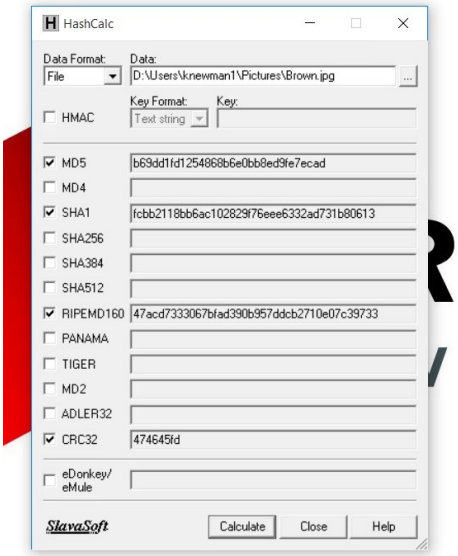


Use HashCalc should be on the VM Desktop) to determine the MD5 and SHA1 message digests for each of the three images downloaded.

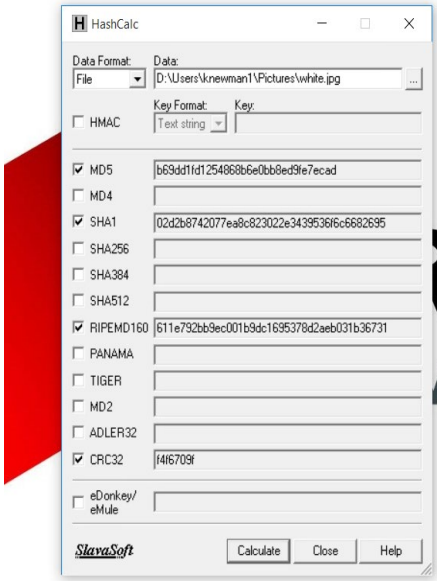
Black.jpg



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.