

## Cipher and John the Ripper Exercise with MEMZ Exercise

### Purpose

This exercise will expose students to different types of ciphers and also introduce them to John the Ripper, a password decryption tool. Students will also be exposed to the devastating effects of a virus on a machine.

### Required

- Kali VM
- Windows 7 VM

### Hand-in

Formal lab write-up in accordance with the Lab Manual Guide.

### Steps

The Caesar Cipher is an older style of substitution encryption. Encrypt the below passwords using a Caesar cipher.

Password	Sdvvzrug
MySecretKey123	<Error>
Root54321	<Error>
*****MyStuff	*****PbVwxii
thisismyfancynewtoughpassword	wklvlpbidqfbqhzwrjksdvvzrug

*Question* What shift number did you use?      3

*Question* Did it work for all above passwords? Why?      No, only works for letters, not numbers or special characters.

*Question* Use an online Caesar decoding tool and decrypt your passwords. Did they take long to decrypt? Why or why not? Does password length matter? Why or why not?

No, it did not take long to decrypt the password. This is because there are only 25 possible shift positions to encrypt using Caesar cipher. Password length does not matter since once the shift number is known, it's a matter of plugging in the letters. Common words make it easier to find a starting point (i.e., and, the).

The One-Time Pad Cipher is another type of password encryption and considered an unbreakable cipher. Create your own one-time pad and encrypt the same passwords. The below example shows a made-up one-time pad used to encrypt the password 'COOKIE.' Notice that although this word contains a duplicate letter, the hash assigned a different letter for each.

25	5	12	8	1	7
----	---	----	---	---	---

```

      C O O K I E
      3 15 15 11 9 5      numerical place in alphabet
+     25 5 12 8 1 7
      28 20 27 19 10 12
-     26 26
      2 20 1 19 10 12
      B T A S J L      hashed password
  
```

Password	
MySecretKey123	
Root54321	
thisismyfancynewtoughpassword	

Search online for password decryption tools and see if you can encrypt your password hashes.

*Question* Were you successful? Why or why not?

Searching online will prove unsuccessful and your passwords secure. This is because of the nature of the one-time pad being random.

*Question* What are advantages and disadvantages of using One-Time Pad Cipher?

**Advantages:** Very secure. The one-time pad is never reused. No obvious patterns making it impossible to crack. Although the receiver must have a copy of the one-time pad for decryption, attacks intercepted will not be able to decrypt without access to the one-time pad.

**Disadvantages:** The one-time pad must be the same length as the message. Must establish a secure method of sharing the one-time pad with the receiver.

*Question* After doing some research, what are some ways to create a new password that is less vulnerable to brute force and dictionary attacks?

**Brute Force Attacks** – vulnerable if 8 characters or less. Should be at least 9 characters plus a symbol.

**Dictionary** – vulnerable if numbers are in sequence (i.e., 12345, 98765). Commonly used words and words frequently associated together are vulnerable. Common letter to character substitutions are vulnerable (i.e., 3 for e, @ for a, 8 for b).

**Best:** Use a combination of 4 uncommon words that are not usually together. Does not have to be uppercase. Pick hard or uncommon words, such as 3 uncommon words and 1 made-up word. Symbols not required, but can add in the middle of a word, not between words.

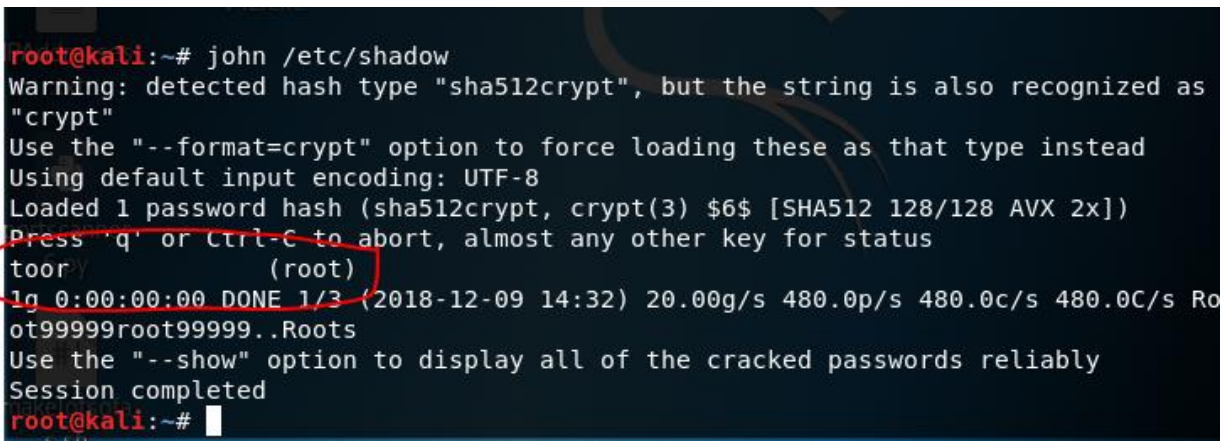
**Examples:** shelfoatmealdistrictshockolate (shockolate is not a real word)  
 shelfoatmealdist&riectshockolate ('&' symbol within a word, not between)

John the Ripper is an open source password recovery tool installed on Kali. For this exercise, you'll be cracking MD5 and SHA1 hashes.

Once in Kali, open the command prompt and type in john. This will show all the commands available in this application.

John is able to retrieve the username and password on your existing system by entering the below command:

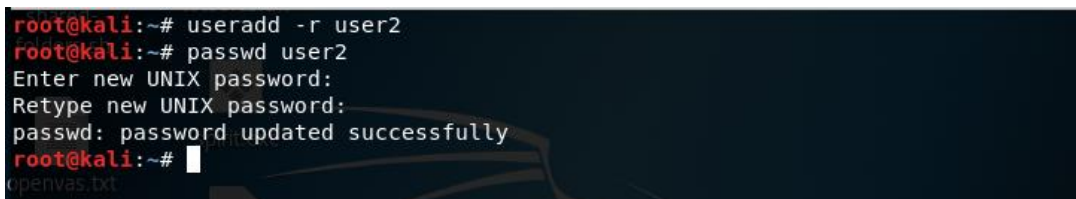
```
john /etc/shadow
```



```
root@kali:~# john /etc/shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
toor (root)
1g 0:00:00:00 DONE 1/3 (2018-12-09 14:32) 20.00g/s 480.0p/s 480.0c/s 480.0C/s Ro
ot99999root99999..Roots
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

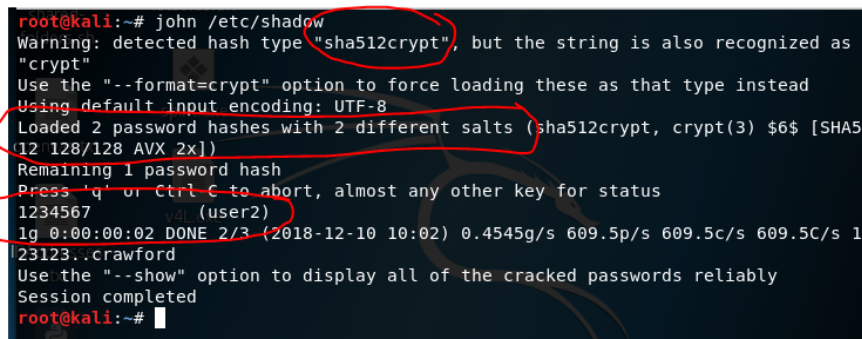
John can also discover the passwords for other users in the system. First, enter the below command to create a new user and password:

```
useradd -r user2
passwd user2
```



```
root@kali:~# useradd -r user2
root@kali:~# passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

Enter the same shadow command used previously to reveal the password of the user2.



```
root@kali:~# john /etc/shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567 (user2)
1g 0:00:00:02 DONE 2/3 (2018-12-10 10:02) 0.4545g/s 609.5p/s 609.5c/s 609.5C/s 1
23123..crawford
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

*Question* The above output reveals several details about the hash. What does the hash type “sha512crypt” signify? Does ‘#’ loaded hashes and ‘#’ different salts display on your output? What does it mean?

John detected the hash type as sha512crypt, which is the hash algorithm used for the encryption. The 2 loaded hashes and 2 different salts means that John has performed the encryption before and will not repeat the encryption for those previous hashes.

John will need password hashes before he can crack them. To hash a list of passwords, create a text file of password hashes either by getting hashes from sources online, or by following the below instructions which will then create a file called ‘target\_hashes.txt.’

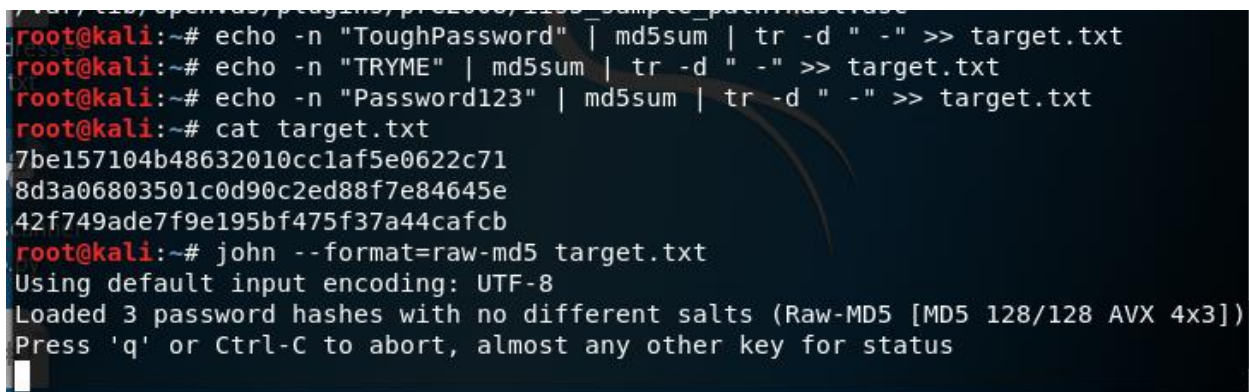
```
echo -n "Password" | md5sum | tr -d " " >> target.txt
```

*Question* Add between 6-8 entries into your text file. What does ‘md5sum’ do? What does tr -d mean?

*Question* John has several formats. To view a list, enter the command `john --list=formats`. What do these formats mean?

The format is the protocol/algorithm type that was used to create the hash. Some available algorithms are md5, blowfish, sha256 and sha512. Providing the format tells John which “reverse” algorithm to use to decrypt to plaintext.

Once the list has been created, you can use the cat command to retrieve the hash list.

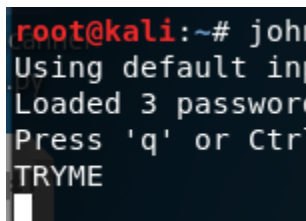


```
root@kali:~# echo -n "ToughPassword" | md5sum | tr -d " " >> target.txt
root@kali:~# echo -n "TRYME" | md5sum | tr -d " " >> target.txt
root@kali:~# echo -n "Password123" | md5sum | tr -d " " >> target.txt
root@kali:~# cat target.txt
7be157104b48632010cc1af5e0622c71
8d3a06803501c0d90c2ed88f7e84645e
42f749ade7f9e195bf475f37a44cafc
root@kali:~# john --format=raw-md5 target.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Now is time for John to crack some password hashes. Since the hashes in the text file are raw-md5 hash, enter the below command:

```
john -format=raw-md5 target.txt
```

Depending on the passwords you used, this process may take a few seconds to several minutes.



```
root@kali:~# john
Using default inp
Loaded 3 password
Press 'q' or Ctr
TRYME
```

**Question** Did all of your passwords get decrypted? Why or why not?

Depending on the hashes in the text file, your passwords may have not been decrypted. Md5 is only one format and success depends on the wordlist that is used to decrypt passwords. John the Ripper includes its own wordlist, which contains a list of guesses, but another wordlist, such as rockyou.txt which is included in Kali can also be used.

Now, try with a SHA-1 hash. Use an online tool for a SHA-1 hash generator and replace your text file content with the SHA-1 hash.

Rerun John, first changing the format: `john --format=raw-sha1 target.txt`

```
root@kali:~# john --format=raw-sha1 target.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
hello          (?)
lg 0:00.00:00 DONE 2/3 (2018-12-09 15:39) 100.0g/s 2400p/s 2400c/s 2400C/s servi
ce..hello
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Repeat above using the sha-256 format.

John's default can be limited, but other wordlists can be included. Wordlists can be added to the command to pull from a larger pile of guesses. Enter the below command which will pull from the 'rockyou' wordlist rather than pulling from John's default wordlist. If Kali isn't able to locate the file, include the complete file path.

`John --format=raw-md5 --wordlist=rockyou.txt target.txt`

```
root@kali:~# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/target.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
```

John will not crack the same password twice. Rerunning the command results in a message stating there are no passwords to crack. To view cracked passwords, type the below command:

`cat /root/.john/john.pot`

```
root@kali:~# cat /root/.john/john.pot
$6$Rw99zZ2B$AZwfboPwM6z2tiBeK.EL74sivucCa8YhCrXGcBoVdeYUGsf8iwNxJkr.wTLDjI5poyga
UcLaWtP/gewQk07jT/:toor
$dynamic_0$dc647eb65e6711e155375218212b3964:Password
$dynamic_0$eb61eead90e3b899c6bcbe27ac581660:HELLO
$dynamic_0$8d3a06803501c0d90c2ed88f7e84645e:TRYME
$dynamic_26$aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d:hello
root@kali:~#
```

You have successfully completed the password decryption portion of the lab.

## MEMZ Exercise **\*\*USE CAUTION\*\***

Having your password cracked is a serious matter and can open a door for malware to take over your machine or network. Other viruses can simply be downloaded inadvertently by visiting a website or opening an email. This exercise will expose students to the effects of a trojan virus on a virtual machine, essentially destroying the machine.

**CAUTION:** This exercise WILL DESTROY the machine. **ONLY USE ON A VM.** Students should exercise caution and ensure they do not have anything valuable on the machine being attacked. It is also a good idea to have a backup VM to later replace the existing VM, which will be not be retrievable. Only perform this exercise in a controlled environment.

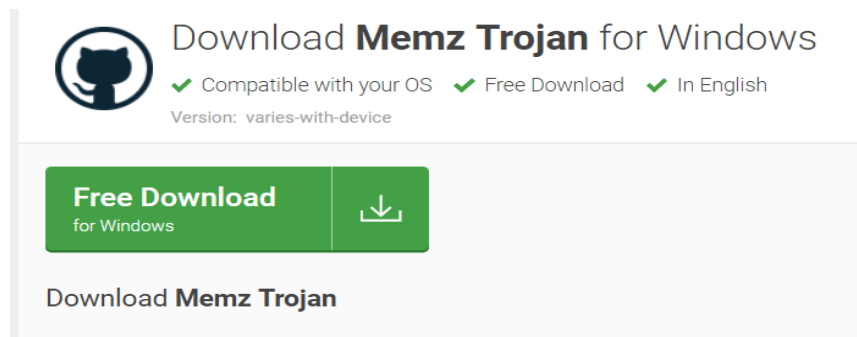
### *Steps*

Open a Windows virtual machine of your choice. For this exercise, Windows 7 was used, but any Windows machine will work.

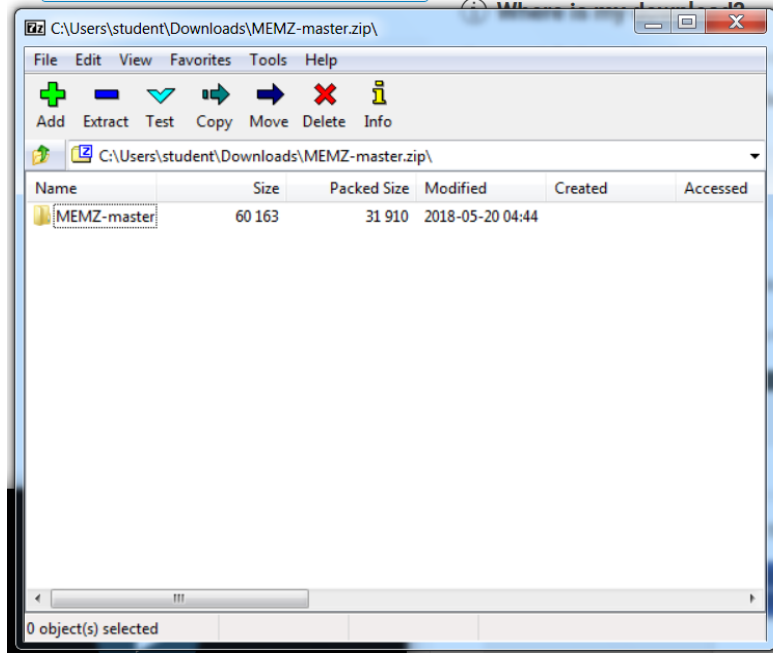
**NOTE: EVERYTHING GOING FORWARD SHOULD BE DONE FROM A VIRTUAL MACHINE**

Open Firefox browser from your VM. Again, use the internet in your VM only, **DO NOT USE YOUR ACTUAL COMPUTER.** Google Chrome and Internet Explorer will attempt to block the malicious file from being downloaded, but Firefox should comply.

First, download MEMZ by searching online. One possible source is <https://memz-trojan.jaleco.com/>.



Search in your downloads folder and move the zipped file to your VMs desktop if desired.



*Question* The zipped file needs to be modified to be executed. Download WinRAR. What does WinRAR do?

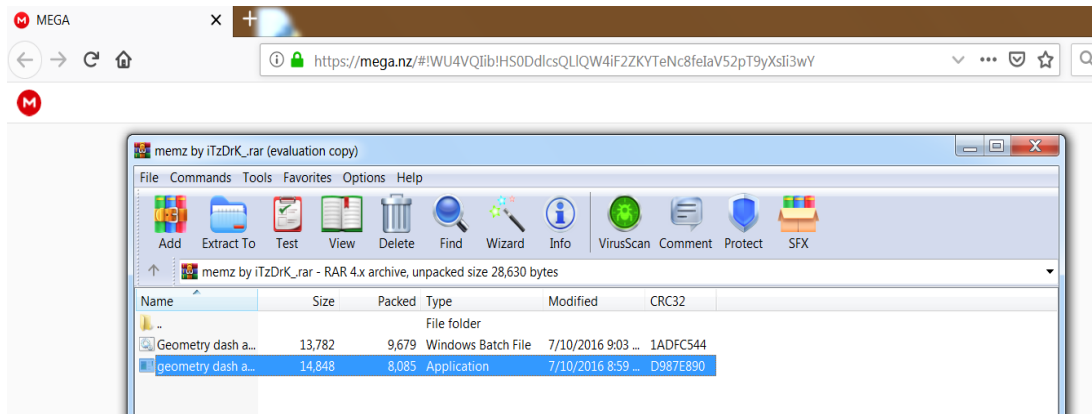
WinRAR is a shareware program that unpacks a zipped file for access and execution. Alternatives can be used, but WinRAR provides a shortcut that provides the user with a file ready to execute.

A screenshot of the WinRAR website's download page. The browser's address bar shows 'https://www.rarlab.com/download.htm'. A cookie notice is visible at the top. The main heading is 'RARLAB WinRAR and RAR archiver downloads'. On the left is a navigation menu with links for Home, RAR, News, Themes, Extras, Downloads, Dealers, Feedback, Partnership, Privacy, and Imprint. The main content area is titled 'English WinRAR and RAR release' and lists various software versions and platforms with blue hyperlinks: WinRAR x86 (32 bit) 5.61, WinRAR x64 (64 bit) 5.61, RAR for Android on Google Play, RAR for Android 5.60 build 63 local copy, RAR 5.61 for Linux, RAR 5.61 for Linux x64, RAR 5.61 for FreeBSD, RAR 5.61 for macOS (64 bit), and WinRAR interface themes.

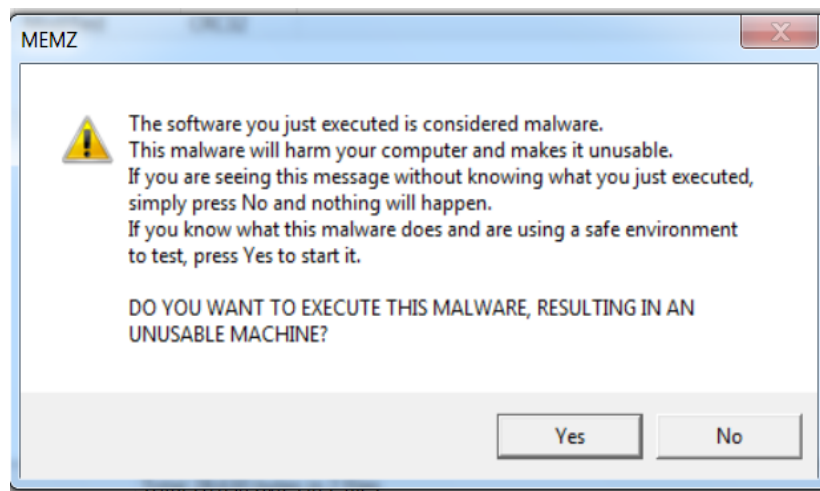
Make sure to select the correct version and then run the program.



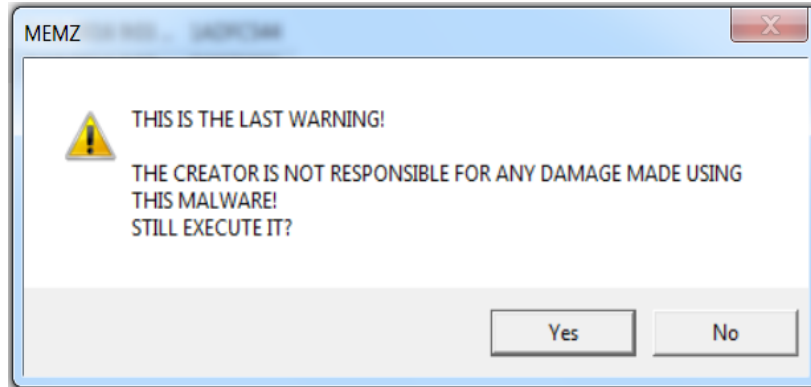
The MEMZ file can now be converted into an executable format displaying two files. Click the file in lowercase.



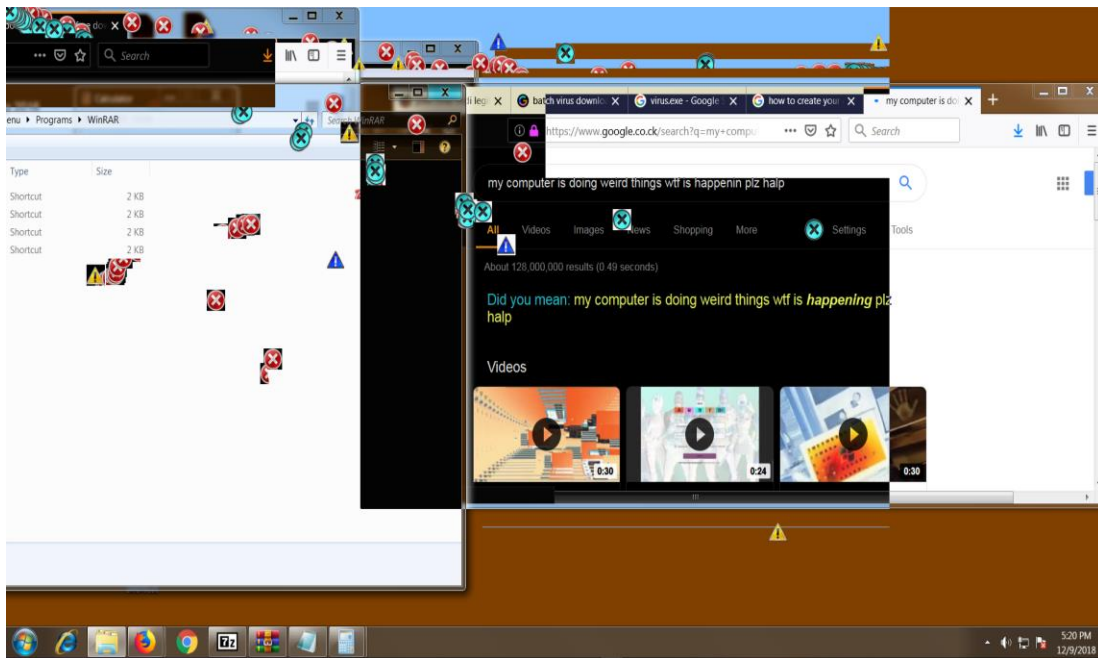
Your virus should now be activated and the VM should respond with several warning messages.

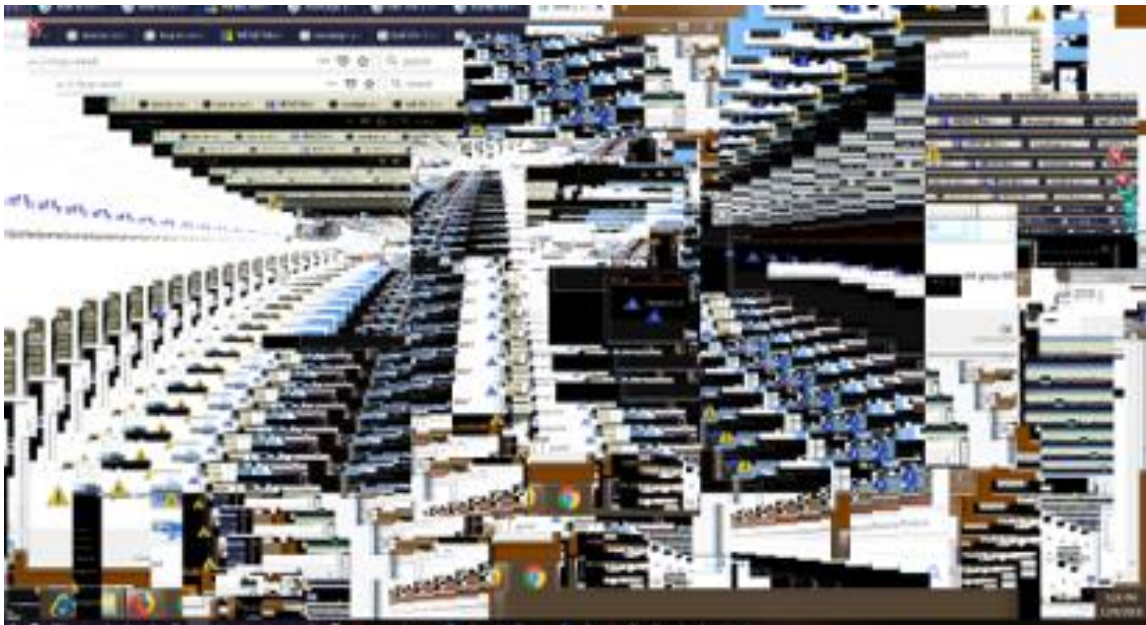
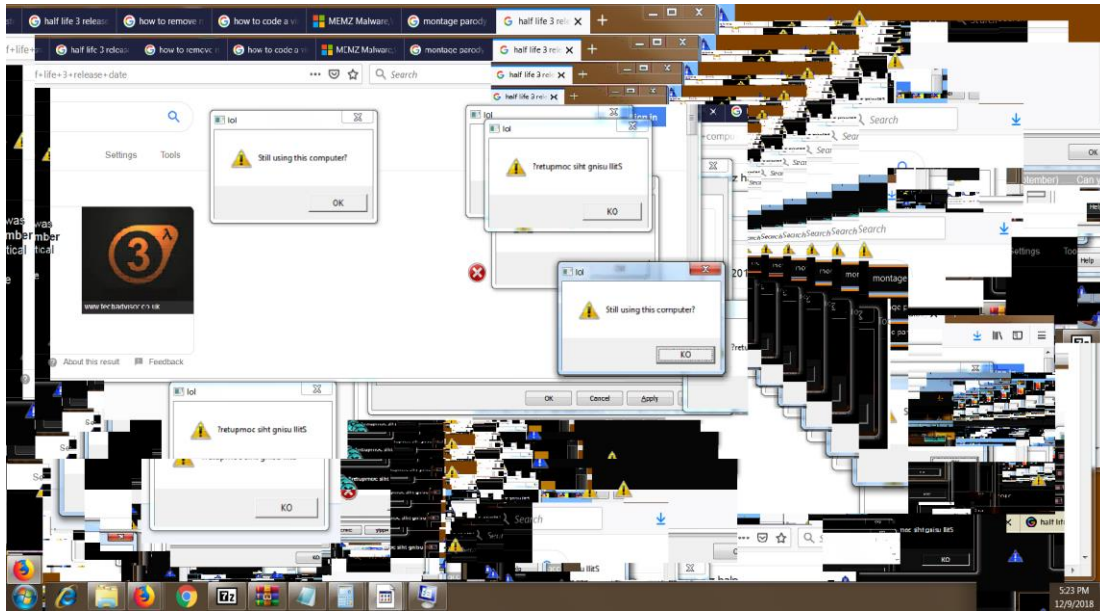


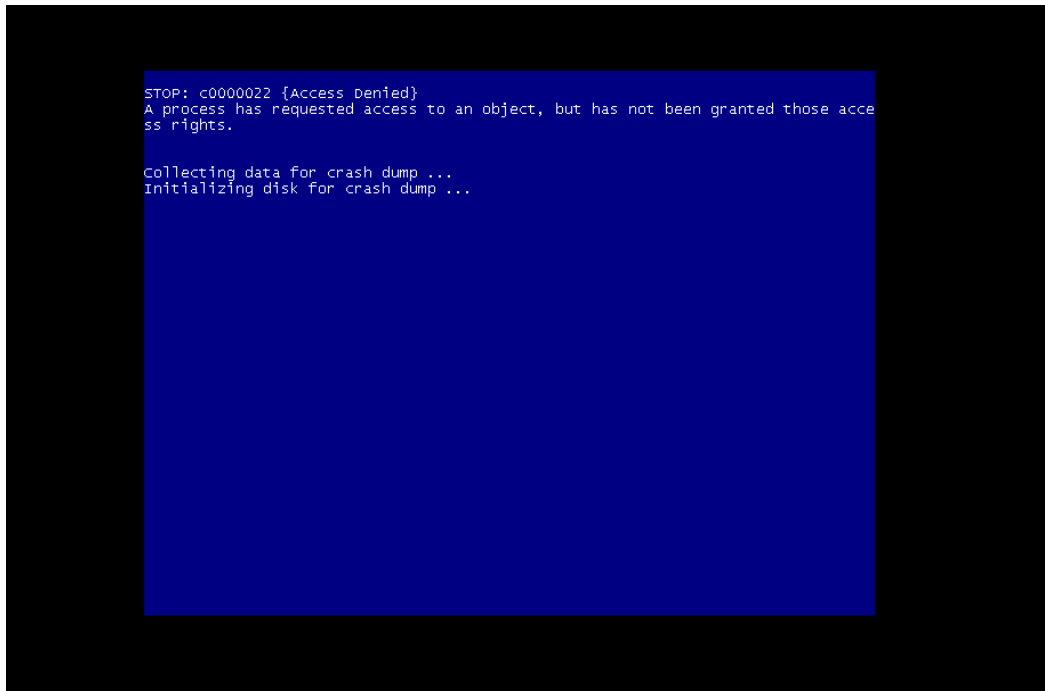
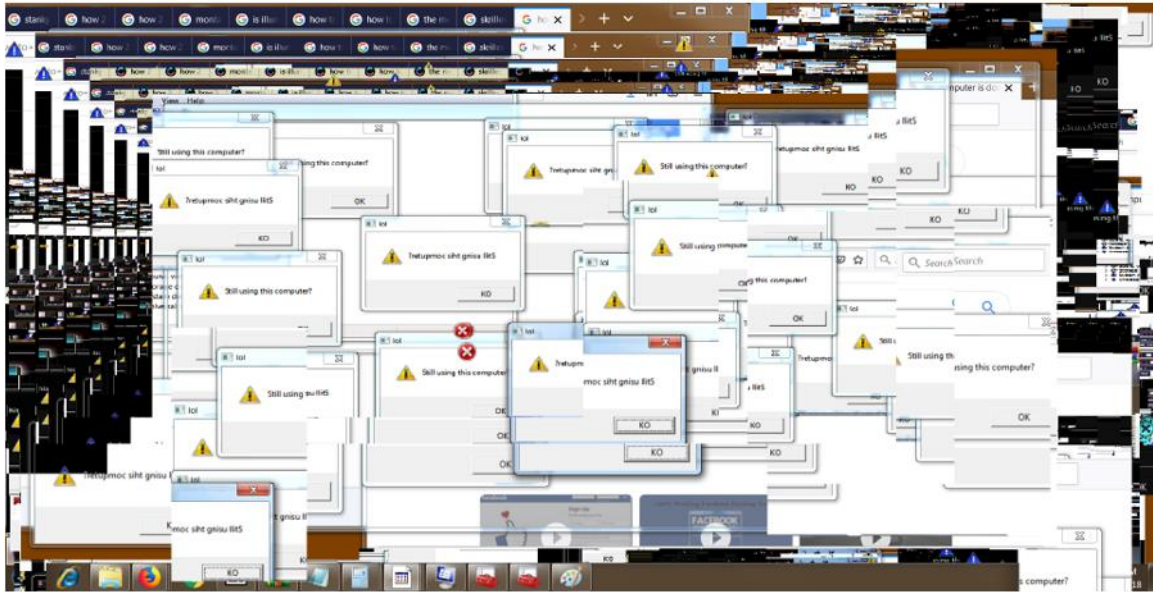




The machine should then display a greeting, signifying that your computer can only be used for a limited time. Attempt to use your machine as the virus takes over rendering it unresponsive to your commands. You have successfully destroyed your Windows machine and completed the lab. The below screenshots show what may happen. Congratulations! Remember that your actual machine is safe and sound, for now.







## References

Hack, T. T. (2017, June 22). *John The Ripper - Tutorial*. Retrieved December 9, 2018, from YouTube: <https://www.youtube.com/watch?v=sZAP8evOiHk>

Techpanther. (2017, April 16). *How to Crack Password using John The Ripper Tool*. Retrieved December 9, 2018, from YouTube: <https://www.youtube.com/watch?v=XIZEHiWsQVk>

Wet. (2017, March 19). *memz.exe on windows 7*. Retrieved December 9, 2018, from YouTube: <https://www.youtube.com/watch?v=rON4G7OnjCM>

Woo, E. (2014, October 31). *The Unbreakable Cipher: One-Time Pad*. Retrieved December 9, 2018, from YouTube: [https://www.youtube.com/watch?v=2\\_w919visH8](https://www.youtube.com/watch?v=2_w919visH8)