
ARL South Cyber Rapid Innovation Group Presents:
Cybersecurity Awareness Workshop Series
WannaCry




Developed by Adriana Escobar Del La Torre & Ana Garcia Ramirez
Advised by Dr. Jaime Acosta and Dr. Salamah Salamah
Estimated time: 1- 1.5 hours

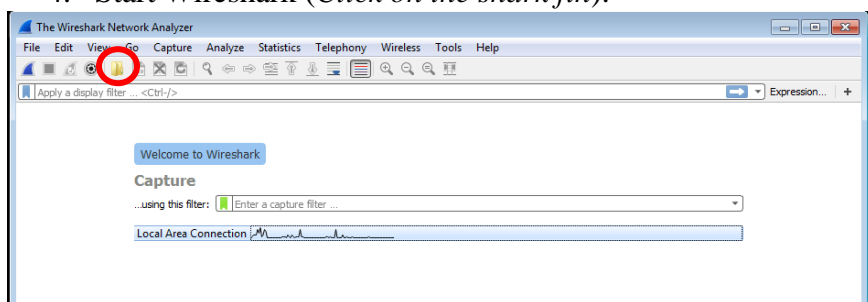
Recently, ransomware has become a well-known and worldwide issue. Victim's computer files are encrypted (garbled up and unreadable) and can only be recovered if a fee, or ransom, is paid within a certain amount of time.

In this exercise, you will execute a series of steps to investigate the WannaCry malware. Your main objective is to uncover the kill switch that will stop this malware from spreading and infecting others.

Activity 1 – You will use Wireshark to analyze traffic and make observations about the behavior of the malware.

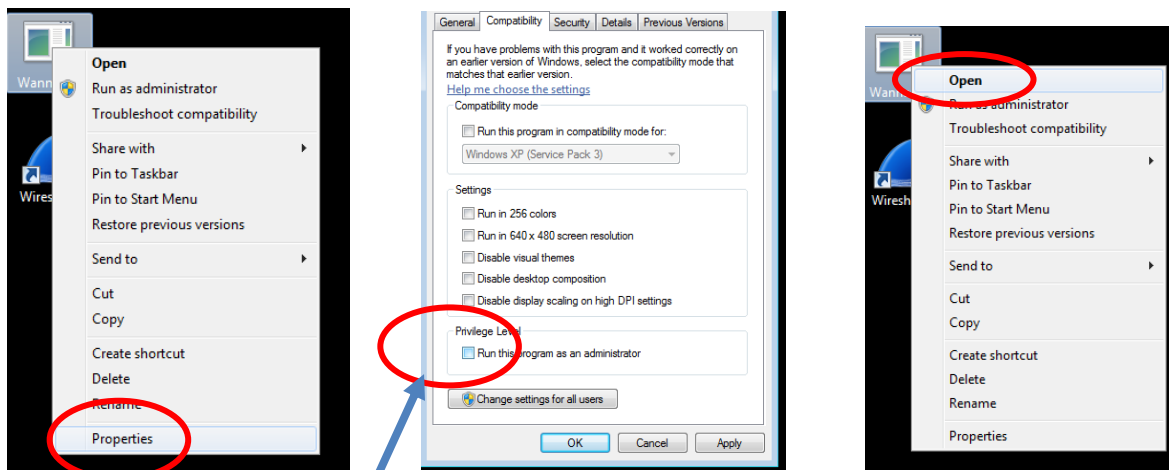
Wireshark is a free and open source network packet analyzer. Wireshark captures network packets and displays the packet data as detailed as possible. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

1. Ensure that you are connected to CIT and then click on the link to the *VictimWin7* machine
2. Locate Wireshark  on the desktop and double click on the icon to open the program.
3. Click on *Local Area Connection*.
4. Start Wireshark (*Click on the shark fin*).



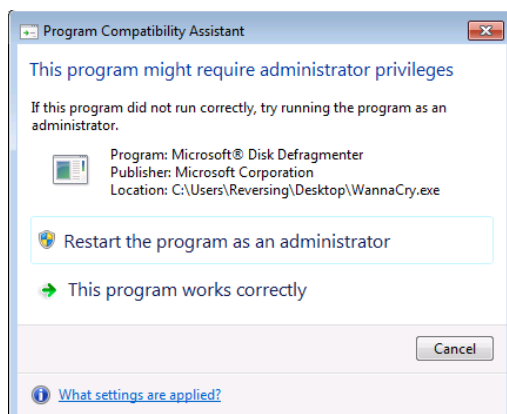
IMPORTANT: Leave Wireshark running throughout the remainder of the exercise.

5. Run WannaCry (it's on your Desktop) **without** administrator privileges as shown below:



Make sure this
is **unchecked**

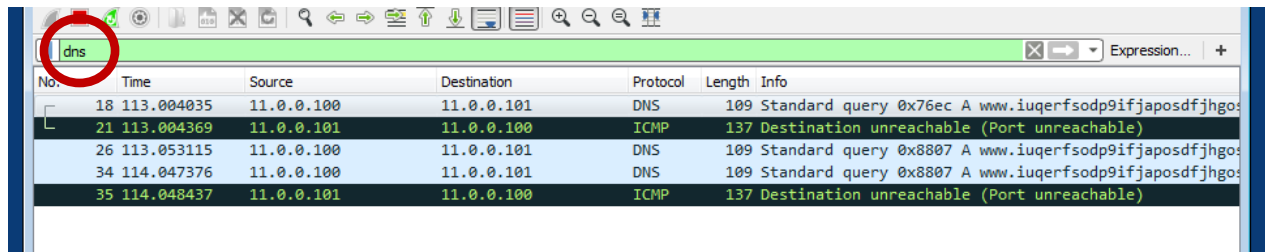
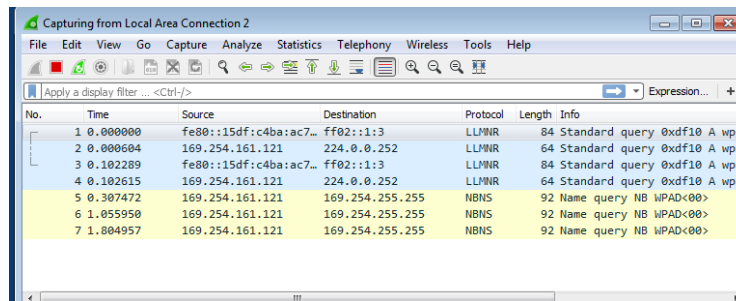
If the following prompt appears, click on “This Program works correctly”:



Note that this will not infect your machine, but you can still observe it trying to communicate with other devices through Wireshark.

Domain Name System packets are used to query a server to obtain the mapping between names (e.g., google.com) to addresses (e.g., 72.14.207.99). These packets may be a good way to identify malware communication channels.

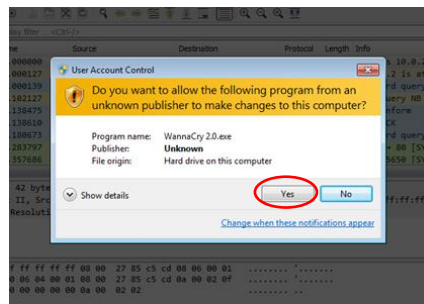
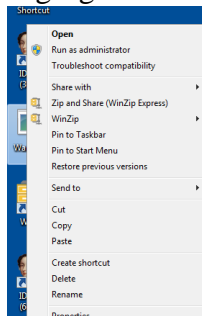
6. In Wireshark, click on the *Filter Tool Bar*, type **dns**, and then press enter to show only Domain Name System packets (see Figures below).



- Click through several DNS packets while observing the packets details (lower window). You should find at least one packet with a suspicious domain that is requested (hint: it starts with **www.**). Write it here.

www._____

- Now run WannaCry **with** administrator privileges. Right click on the WannaCry icon and select **Run as administrator**. When prompted, press the Yes button as shown in the following figures.



- After a short while, you will notice that a file on the desktop has been encrypted (this may take up to 5 minutes). Write down the name of this file.

Before two devices can communicate, similar to sending a letter through the mail, they must know the other's physical addresses. This is accomplished by sending data in the form of **address resolution protocol (ARP)** packets.

10. In Wireshark, clear out the existing filter and then apply a filter to view only **ARP** packets (use arp as your filter string).

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
38	45.171091	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.1? Tell 11.0.0.100
39	45.196386	11.0.0.100	11.0.0.255	NBNS	92	Name query NB WPAD<00>
40	45.227859	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.2? Tell 11.0.0.100
41	45.290323	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.3? Tell 11.0.0.100
42	45.352889	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.4? Tell 11.0.0.100
43	45.424112	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.5? Tell 11.0.0.100
44	45.477742	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.6? Tell 11.0.0.100
45	45.540335	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.7? Tell 11.0.0.100
46	45.602765	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.8? Tell 11.0.0.100
47	45.666319	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.9? Tell 11.0.0.100
48	45.727776	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.10? Tell 11.0.0.100
49	45.790229	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.11? Tell 11.0.0.100
50	45.883739	11.0.0.100	11.0.0.255	NBNS	92	Name query NB WPAD<00>
51	45.946239	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.1? Tell 11.0.0.100
52	45.946274	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.2? Tell 11.0.0.100
53	45.946386	PcsCompu_a2:cf:46	Broadcast	ARP	42	Who has 11.0.0.3? Tell 11.0.0.100

11. Based on your observations (look at the **Info** column in Wireshark), in your own words, do your best to briefly describe what you think the malware is trying to do:

The **Server Message Block protocol (SMB)** is a protocol that let's devices share files over a network. It was originally specified by Microsoft, IBM, and Intel.

12. Clear the current filter and apply a filter to show only **smb** packets.

Wireshark provides packet symbols to identify packets that are related. Click on a line of the "Packet List" pane to show the packet symbol.

First packet in a conversation.

Part of the selected conversation.

Not part of the selected conversation.

Last packet in a conversation.

Request.

Response.

The selected packet acknowledges this packet.

The selected packet is a duplicate acknowledgement of this packet.

The selected packet is related to this packet in some other way, e.g. as part of reassembly.

13. Look at the SMB traffic flow and do your best to give a high-level explanation of what the malware is trying to do.

*Hint:
into the
column
packet.*

No.	Time	Source	Destination	Protocol	Length	Info
8	71.884998	11.0.0.100	11.0.0.255	BROWSER	251	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
329	123.453567	11.0.0.100	11.0.0.101	SMB	142	Negotiate Protocol Request
351	124.185232	11.0.0.101	11.0.0.100	SMB	185	Negotiate Protocol Response
352	124.185609	11.0.0.100	11.0.0.101	SMB	157	Session Setup AndX Request, User: .\
353	124.261511	11.0.0.101	11.0.0.100	SMB	175	Session Setup AndX Response
354	124.261929	11.0.0.100	11.0.0.101	SMB	126	Tree Connect AndX Request, Path: \\11.0.0.101\IPC\$
355	124.262656	11.0.0.101	11.0.0.100	SMB	93	Tree Connect AndX Response, Error: Non specific error code
356	124.262908	11.0.0.100	11.0.0.101	SMB PL	132	PeeKNamedPipe Request, FID: 0x0000
357	124.263694	11.0.0.101	11.0.0.100	SMB	93	Trans Response, Error: TID invalid
444	127.266897	11.0.0.100	11.0.0.101	SMB	191	Negotiate Protocol Request
445	127.266889	11.0.0.101	11.0.0.100	SMB	173	Negotiate Protocol Response
446	127.267059	11.0.0.100	11.0.0.101	SMB	194	Session Setup AndX Request, User: anonymous
448	127.268139	11.0.0.101	11.0.0.100	SMB	251	Session Setup AndX Response
449	127.268415	11.0.0.100	11.0.0.101	SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$

*Look
Info
of each*

14. Wait until the following Window appears. (This may take up to 5 minutes)



15. Open Windows Explorer and list a few file types that are encrypted and some that are not encrypted. The system will be slow... keep in mind that malware is running.

16. What is the malware using to decide which files to encrypt?


Activity 2 – You will use binary analysis with the IDA Pro tool to identify the ransomware’s kill switch by analyzing low-level code. You will then implement and test the kill switch that stops the ransomware from infecting your system.

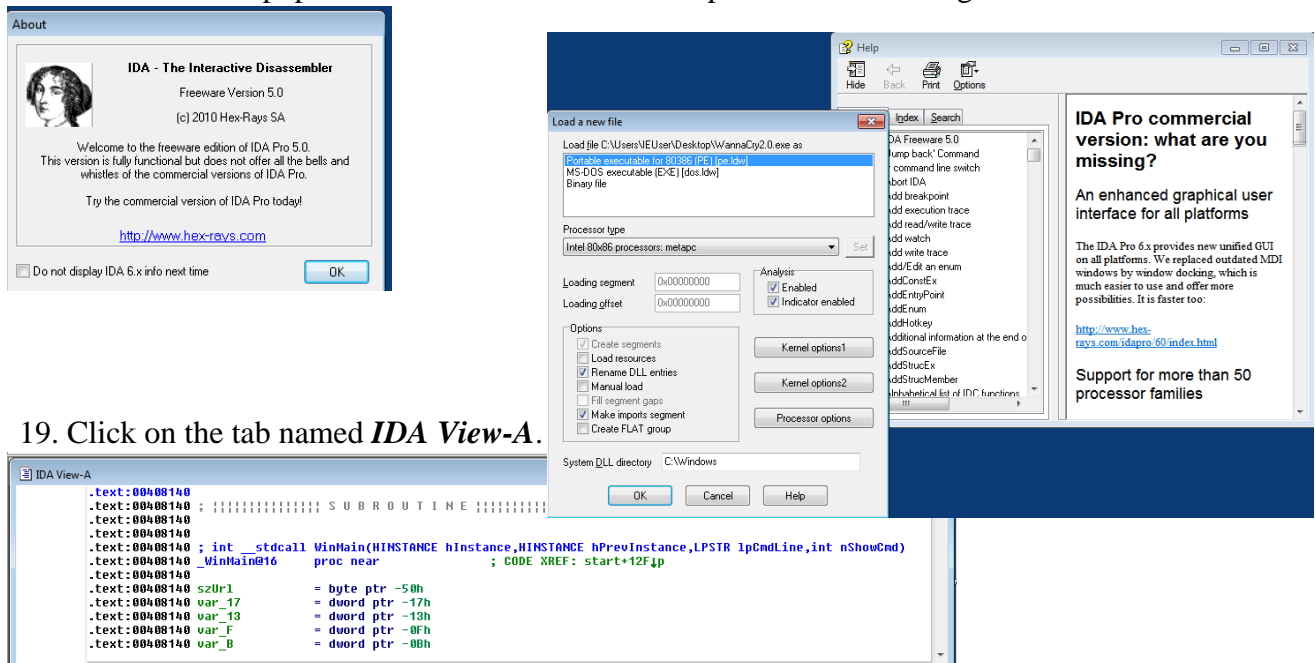
Part 1- Binary analysis using IDA Pro.

*****IDA

A Pro is a combination of disassembler and debugger. It facilitates both static and dynamic analysis. It is a powerful tool commonly used by professionals to perform malware analysis.

17. Return to the CIT home screen (click the back button on your host’s browser. Now click on the link to open the *CleanWin7*

18. Locate IDA Pro  and drag the binary named *WannaCry* onto the IDA Pro icon. Click *OK* on the two pop-out windows and *Close* in Help as shown in the figures below.



19. Click on the tab named *IDA View-A*.

*****A
kill switch is a mechanism used to shut down or disable machinery of a device or program. The importance of finding a ransomware’s kill switch is to prevent it from spreading. Keep in mind that not every malware has a kill switch.

20. Scroll down until you find the domain name (the “www...” string that you found in Activity 1, Step 7).

```

ext:00408140 nShowCmd = dword ptr 10h
ext:00408140
ext:00408140 sub esp, 50h
ext:00408143 push esi
ext:00408144 push edi
ext:00408145 mov ecx, 0Eh
ext:0040814A mov esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdfjhgosurij"
ext:0040814F lea edi, [esp+58h+szUrl]
ext:00408153 xor eax, eax
ext:00408155 rep movsd
ext:00408157 movsb
ext:00408158 mov [esp+58h+var_17], eax

```

In the low level (or assembly) code, the following imports (names written in pink) are used to interact with the Internet. The Windows Internet (WinINet) application programming interface (API) enables applications to interact with FTP, and HTTP protocols to access Internet resources. These are some of the functions that make up the API.

InternetOpen function initializes an application's use of the WinINet functions.

InternetOpenUrlA function opens a resource specified by a complete FTP or HTTP URL.

InternetCloseHandle function closes a single Internet handle. Returns TRUE if the handle is successfully closed, or FALSE otherwise.

21. Scroll down and find the functions to access the network in the code.

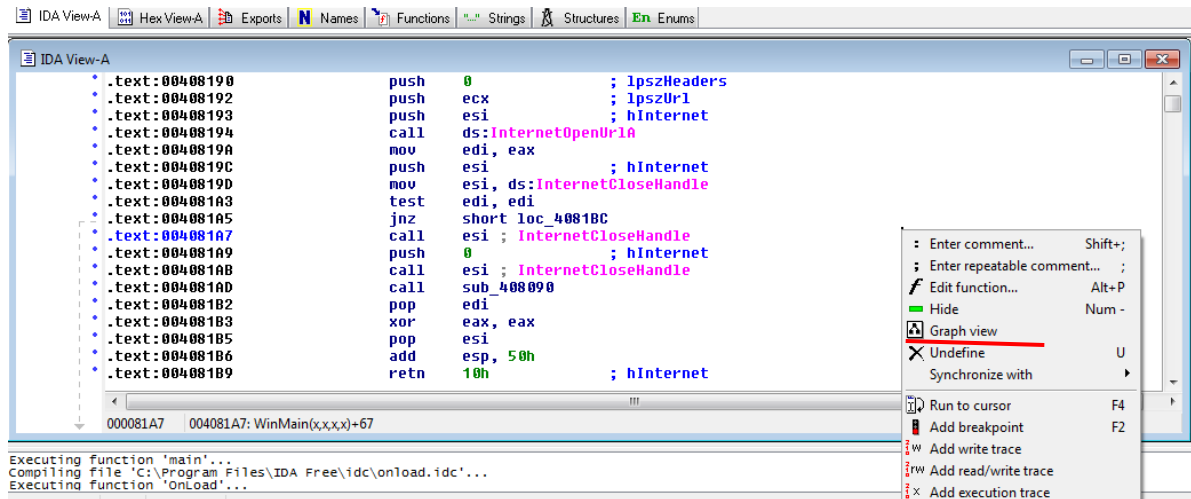
```

.text:00408174 push 1 ; dwAccessType
.text:00408176 push eax ; lpzAgent
.text:00408177 mov [esp+6Ch+var_1], al
.text:0040817B call ds:InternetOpenA
.text:00408181 push 0 ; dwContext
.text:00408183 push 84000000h ; dwFlags
.text:00408188 push 0 ; dwHeadersLength
.text:0040818A lea ecx, [esp+64h+szUrl]
.text:0040818E mov esi, eax
.text:00408190 push 0 ; lpzHeaders
.text:00408192 push ecx ; lpzUrl
.text:00408193 push esi ; hInternet
.text:00408194 call ds:InternetOpenUrlA
.text:0040819A mov edi, eax
.text:0040819C push esi ; hInternet

```

Another way to find these functions is to view the Imports tab and look for the names of the functions and then right-click and select “jump to xref” This will list all places in the code that reference the function.

22. Right click on the IDA View-A window and click on graph view.



Some common instructions found in assembly are:

call jumps to another **block of code**; when execution of that block is complete, the program execution **will return**.

jmp jumps to another **block of code**; when execution of that block is complete, the program execution **does not need to return**.

test executes a logical AND (typically used for value comparisons)

jnz jumps to another block of code **if** a condition is met: **result** of the **previous instruction** is **not zero**.

mov instruction **moves data** from one location to another.

push **adds** a value **to the stack**.

pop **removes** value **from** the top of the **stack** into a register or memory address.

23. Focus on **call** instructions and the **pink function names** and then do your best to generally explain what is happening in the code.

24. Look at the subroutines after the conditional jump (follow the two arrows to below the **jnz** instruction). Which subroutine (or **block**) is the one that continues with the encryption and which one stops before encryption occurs? Explain why.

Hint: See the code within functions by double-clicking on the function names. You can go back by pressing **ESC** or the back arrow.

```

mov     esi, ds:InternetCloseHandle
test    edi, edi
jnz     short loc_4081BC

```

25. B
a
s
e
d

o
n

```

call    esi ; InternetCloseHandle
push    0 ; hInternet
call    esi ; InternetCloseHandle
call    sub_408090
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h ; hInternet

```

```

loc_4081BC:
call    esi ; InternetCloseHandle
push    edi ; hInternet
call    esi ; InternetCloseHandle
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h
_WinMain@16 endp

```


what you observed so far, do your best to guess what would prevent the encryption, that is, what should we do to reach the **block** that **stops** the malware; what is *the kill switch*?
(Remember you can always ask one of the coordinators to help)

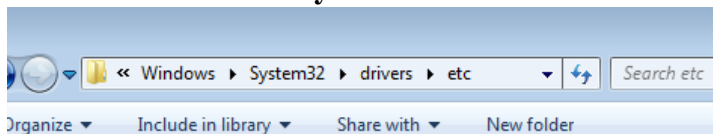
Part 2 - Set up the kill switch

There is a file named *hosts* on Windows systems. This is a text file that contains mappings from hostnames to IP addresses

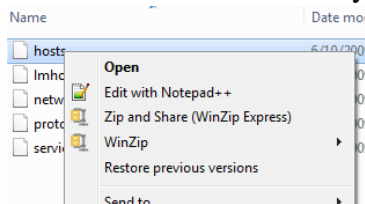
(think of as a stored copy of a Domain Name System that maps google.com -> 72.14.207.99)

26. Add a mapping as shown in the following.

- Open *File Explorer* .
- Navigate to the folder with the hosts file by entering
%WINDIR%/system32/drivers/etc into the navigation bar.



- Edit the hosts file by right clicking and selecting *notepad++*



- Add a mapping between google.com and the loopback address: **127.0.0.1** This is a special address used to communicate within your own machine.

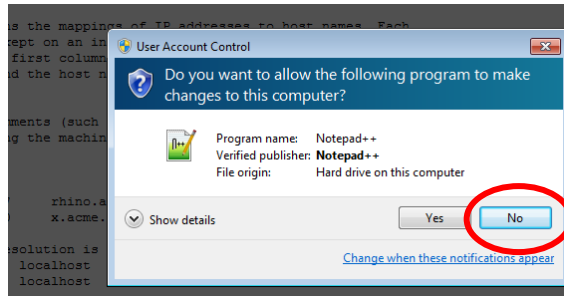
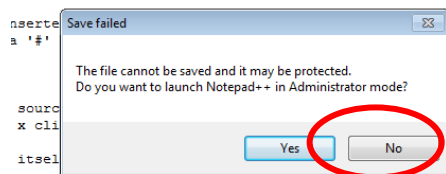
```

18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22 127.0.0.1 google.com
23 127.0.0.1 www.google.com
24

```

- e. Save the *hosts* file. If you received a *Save failed* prompt, press the Yes button as shown below.

to host names. Each
IP address should
corresponding host name.
rated by at least one



- f. Navigate to google.com (this may take 1-2 minutes). You will see the page returned from your own machine's web server (note that this is *not* Google's web server).



27. Now, set up the kill switch by adding a mapping to the address you found in Activity 1, Step 7 using the hosts file.

28. After you set up the kill switch, run the malware as an administrator. Read the following hint before you execute this step.

Hint: Before running the malware make sure the domain works. Go to the site and check that it accesses the local host. As an additional safeguard make sure you also take a snapshot of the machine state by going into your VirtualBox's VM Window menu into Machine > Take Snapshot.

Alternatively you can enter the Host (Windows) key + T to take a snapshot.

If done correctly, your system will not be encrypted. If done incorrectly... well, you know... If you took a snapshot and you incorrectly followed the steps you can go back to the previous machine state by closing your Virtual Machine Window, and starting it up again, VirtualBox should restore your machine state automatically.

Uber Question:

- Why do you think this ransomware have a kill switch?

This concludes the analysis of the malware WannaCry 2.0

Please raise your hand and let the coordinators know that you've completed Activity 2.