Behavioral Analysis

(Watching the malware infect your computer)

What is Behavioral Analysis?

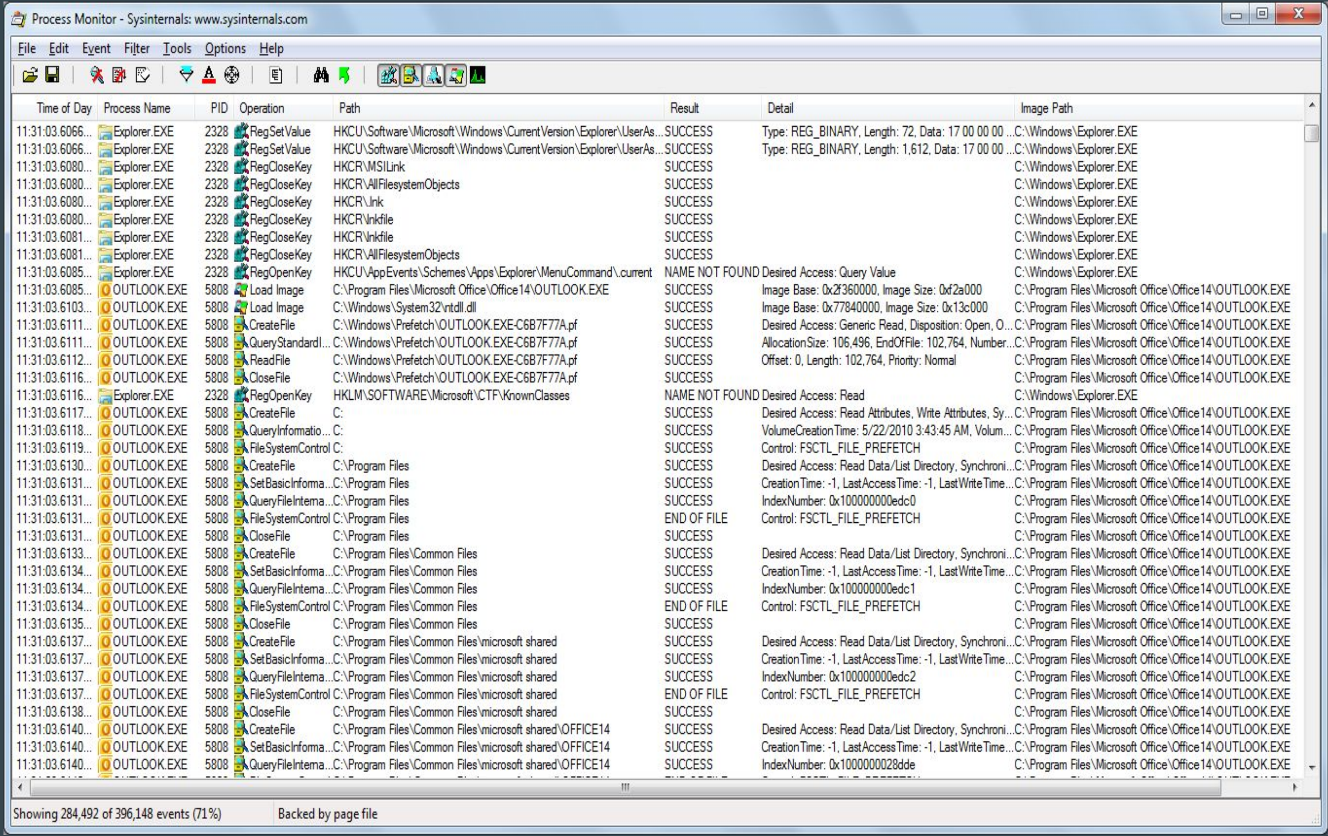
- Typically performed after performing a static properties analysis through tools such as strings (our favorite), PeStudio (for windows), or pescanner (for linux).
- It involves purposely running malware on your computer with proper monitoring tools in place to analyze what happens to your system.
- At first you give the malware limited resources, determine what happened, then slowly give it more resources.
- “The key is little by little, step by step”
- You should always be doing this from an isolated VM environment

Tools

- Windows:
  - Process Monitor
  - Regshot
  - Process Hacker
  - ProcDOT
  - Capture BAT
  - Noriben
- Linux:
  - Wireshark
  - httpd
  - fakedns

Process Monitor

- Tool that monitors anything and everything that processes do.
- This includes registry manipulation and file creation



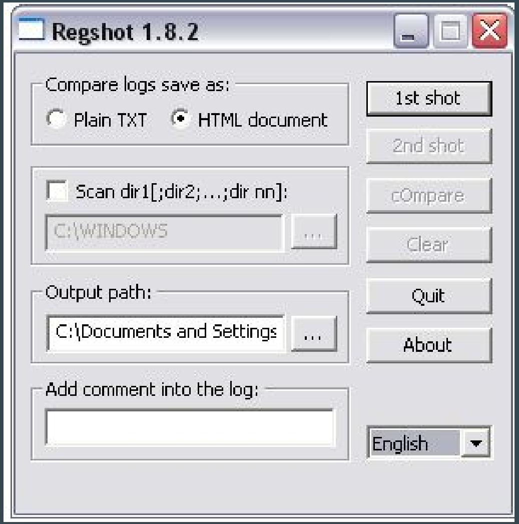
Time of Day	Process Name	PID	Operation	Path	Result	Detail	Image Path
11:31:03.6066...	Explorer.EXE	2328	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 17 00 00 00 ...	C:\Windows\Explorer.EXE
11:31:03.6066...	Explorer.EXE	2328	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs...	SUCCESS	Type: REG_BINARY, Length: 1,612, Data: 17 00 00 ...	C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\MSILink	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\.lnk	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6080...	Explorer.EXE	2328	RegCloseKey	HKCR\lnkfile	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6081...	Explorer.EXE	2328	RegCloseKey	HKCR\lnkfile	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6081...	Explorer.EXE	2328	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS		C:\Windows\Explorer.EXE
11:31:03.6085...	Explorer.EXE	2328	RegOpenKey	HKCU\AppEvents\Schemes\Apps\Explorer\MenuCommand\.current	NAME NOT FOUND	Desired Access: Query Value	C:\Windows\Explorer.EXE
11:31:03.6085...	OUTLOOK.EXE	5808	Load Image	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE	SUCCESS	Image Base: 0x2f360000, Image Size: 0xf2a000	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6103...	OUTLOOK.EXE	5808	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77840000, Image Size: 0x13c000	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6111...	OUTLOOK.EXE	5808	CreateFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, O...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6111...	OUTLOOK.EXE	5808	QueryStandardI...	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	AllocationSize: 106,496, EndOfFile: 102,764, Number...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6112...	OUTLOOK.EXE	5808	ReadFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS	Offset: 0, Length: 102,764, Priority: Normal	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6116...	OUTLOOK.EXE	5808	CloseFile	C:\Windows\Prefetch\OUTLOOK.EXE-C6B7F77A.pf	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6116...	Explorer.EXE	2328	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: Read	C:\Windows\Explorer.EXE
11:31:03.6117...	OUTLOOK.EXE	5808	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Sy...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6118...	OUTLOOK.EXE	5808	QueryInformatio...	C:	SUCCESS	VolumeCreationTime: 5/22/2010 3:43:45 AM, Volum...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6119...	OUTLOOK.EXE	5808	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6130...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files	SUCCESS	IndexNumber: 0x100000000edc0	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6131...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6133...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files	SUCCESS	IndexNumber: 0x100000000edc1	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6134...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files\Common Files	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6135...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files\Common Files	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files\microsoft shared	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files\microsoft shared	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files\microsoft shared	SUCCESS	IndexNumber: 0x100000000edc2	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6137...	OUTLOOK.EXE	5808	FileSystemControl	C:\Program Files\Common Files\microsoft shared	END OF FILE	Control: FSCTL_FILE_PREFETCH	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6138...	OUTLOOK.EXE	5808	CloseFile	C:\Program Files\Common Files\microsoft shared	SUCCESS		C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	CreateFile	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	Desired Access: Read Data/List Directory, Synchroni...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	SetBasicInforma...	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime...	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE
11:31:03.6140...	OUTLOOK.EXE	5808	QueryFileInterna...	C:\Program Files\Common Files\microsoft shared\OFFICE14	SUCCESS	IndexNumber: 0x1000000028dde	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE

Showing 284,492 of 396,148 events (71%)

Backed by page file

Regshot & Process Hacker

- Regshot allows you to take a snapshot of the registry before and after you infect your system, showing what has changed.
- Process Hacker is an extended version of task manager.
  - It shows the parent of each process
  - It gives extended information about the process
  - It can easily kill any process



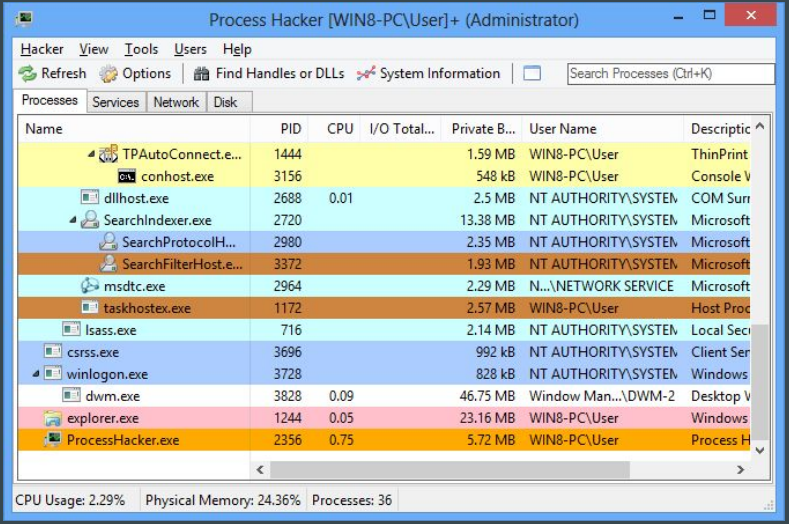
Compare logs save as: ○ Plain TXT ● HTML document

□ Scan dir1[;dir2;...;dir nn]: C:\WINDOWS ...

Output path: C:\Documents and Settings ...

Add comment into the log:

English



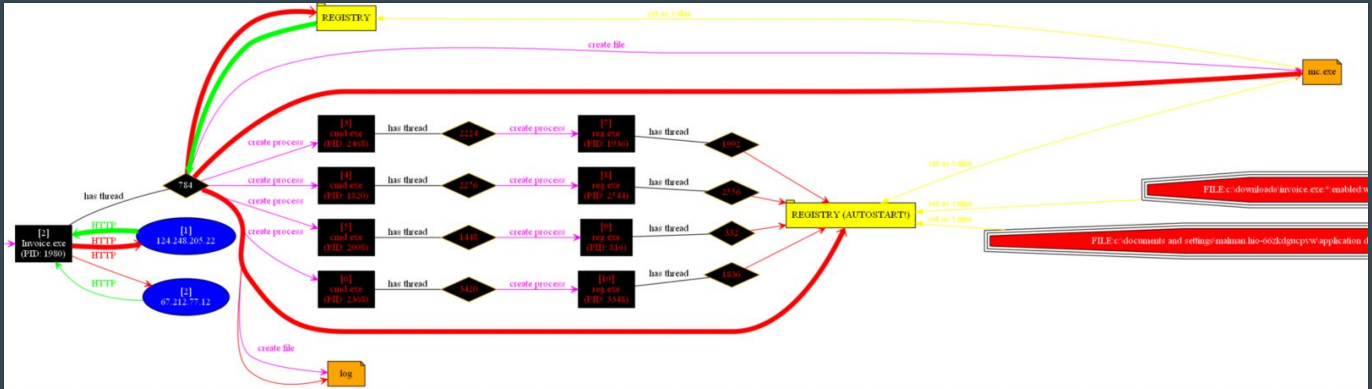
Process Hacker [WIN8-PC\User]+ (Administrator)

Name	PID	CPU	I/O Total...	Private B...	User Name	Descriptic
TPAutoConnect.e...	1444			1.59 MB	WIN8-PC\User	ThinPrint
conhost.exe	3156			548 kB	WIN8-PC\User	Console V
dllhost.exe	2688	0.01		2.5 MB	NT AUTHORITY\SYSTEM	COM Surr
SearchIndexer.exe	2720			13.38 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchProtocolH...	2980			2.35 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchFilterHost.e...	3372			1.93 MB	NT AUTHORITY\SYSTEM	Microsoft
msdtc.exe	2964			2.29 MB	N...\NETWORK SERVICE	Microsoft
taskhostex.exe	1172			2.57 MB	WIN8-PC\User	Host Proc
lsass.exe	716			2.14 MB	NT AUTHORITY\SYSTEM	Local Sec
csrss.exe	3696			992 kB	NT AUTHORITY\SYSTEM	Client Ser
winlogon.exe	3728			828 kB	NT AUTHORITY\SYSTEM	Windows
dwm.exe	3828	0.09		46.75 MB	Window Man...\DWM-2	Desktop V
explorer.exe	1244	0.05		23.16 MB	WIN8-PC\User	Windows
ProcessHacker.exe	2356	0.75		5.72 MB	WIN8-PC\User	Process H

CPU Usage: 2.29% | Physical Memory: 24.36% | Processes: 36

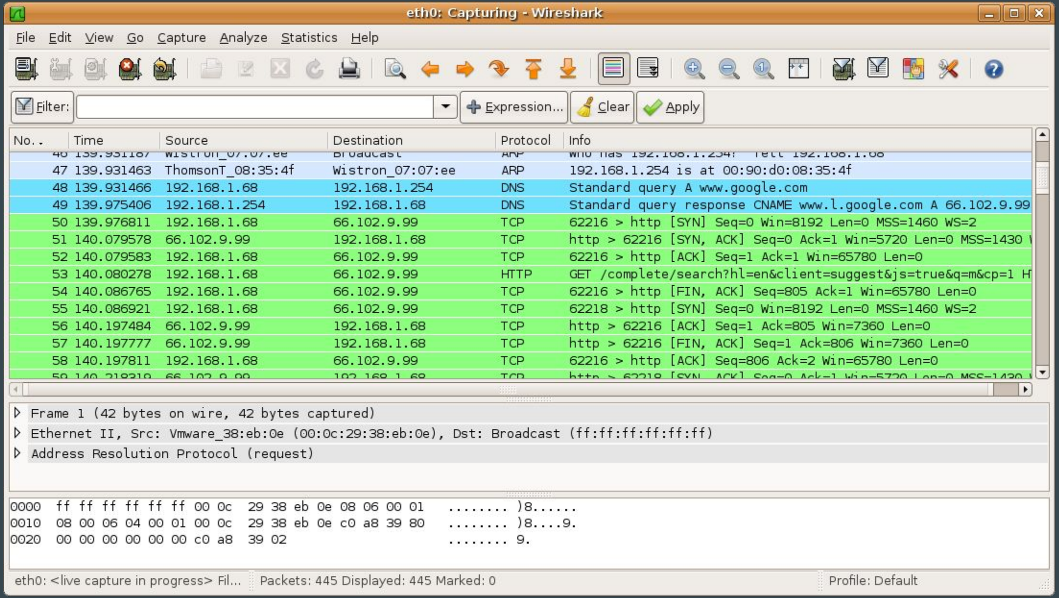
ProcDOT & Noriben & Capture BAT

- ProcDOT will create a beautiful flowchart/graph of the executable. It basically shows everything that happens when you run the program.
- Noriben is a python tool that will look for indicators of compromise and log them.
- Capture BAT is a powerful command line (hah) tool that will monitor registry changes and generate a pcap of the network traffic, which can be analyzed later.



Linux Tools

- httpd can be used to simulate a web server if the malware tries to reach out to a site
- fakedns can be used in conjunction with httpd in order to resolve any hostnames. This gives malware the illusion of connecting to the outside.
- Wireshark - the tool for network captures



```
No. .  Time        Source            Destination      Protocol Info
  46 139.931187  Wistron_07:07:ee  Broadcast        ARP      Who has 192.168.1.254?  Tell 192.168.1.68
  47 139.931463  ThomsonT_08:35:4f Wistron_07:07:ee ARP      192.168.1.254 is at 00:90:d0:08:35:4f
  48 139.931466  192.168.1.68      192.168.1.254    DNS      Standard query A www.google.com
  49 139.975406  192.168.1.254     192.168.1.68     DNS      Standard query response CNAME www.l.google.com A 66.102.9.99
  50 139.976811  192.168.1.68      66.102.9.99      TCP      62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  51 140.079578  66.102.9.99       192.168.1.68     TCP      http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
  52 140.079583  192.168.1.68      66.102.9.99      TCP      62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
  53 140.080278  192.168.1.68      66.102.9.99      HTTP     GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
  54 140.086765  192.168.1.68      66.102.9.99      TCP      62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
  55 140.086921  192.168.1.68      66.102.9.99      TCP      62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  56 140.197484  66.102.9.99       192.168.1.68     TCP      http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
  57 140.197777  66.102.9.99       192.168.1.68     TCP      http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
  58 140.197811  192.168.1.68      66.102.9.99      TCP      62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
  59 140.218319  66.102.9.99       192.168.1.68     TCP      http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

BEHAVIORAL EXAMPLE

QUESTIONS?