School of

#### Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

### CYBR 473 T1 2023 Malware and Reverse Engineering

#### **Basic Dynamic Analysis**

Chapter 3: "Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software", Michael Sikorski and Andrew Honig, 2012





## Tweaking an Analysis VM

- Disable Hidden Extensions
- Show Hidden Files and Folders
- Disable ASLR
- Disable Windows Firewall
- Disable Windows Defender
- Mimic an End-User System
  - $\circ$  Disk size
  - $\circ$  RAM
  - Install software used by most end users
  - $\circ~$  Copy over dummy files
  - Populate file history

## MONITORING WITH PROCESS MONITOR

.

#### **Process Monitor**

- Monitors registry, file system, network, process, and thread activity
- All recorded events are kept, but you can <u>filter</u> the display to make it easier to find items of interest
- Don't run it too long, or it will fill up all RAM and <u>crash</u> the machine

### Launching Calc.exe

• Many, many events recorded

👌 Process Monitor - Sysinternals: www.sy	sinternals.com				
<u>File Edit Ev</u> ent Fi <u>l</u> ter <u>T</u> ools <u>O</u> ptio	ons <u>H</u> elp				
😅 🖬   🍳 👺 🖾   🗢 🔺 6	9   E   M 📕				
Time of Day Process Name	PID Operation	Path	Result	Detail	-
1:17:48.5991893 PM Explorer.EXE 1:17:48.5992018 PM Explorer.EXE 1:17:48.5998061 PM Explorer.EXE	3188 🍂 RegOpen Key 3188 戱 RegClose Key 3188 🛃 Close File	HKLM\Software\Microsoft\Windows\CurrentVersion\ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi C:\Windows\winsxs\x86_microsoft.windows.common	SUCCESS SUCCESS SUCCESS	Desired Access: Query Value	
1:17:48.6001092 PM calc.exe 1:17:48.6001273 PM calc.exe 1:17:48.6001350 PM calc.exe	2072 KRegOpenKey 2072 KRegQueryValue 2072 KRegCloseKey	HKLM\Software\Microsoft\Windows\Windows Error HKLM\SOFTWARE\Microsoft\Windows\Windows Err. HKLM\SOFTWARE\Microsoft\Windows\Windows Err.	SUCCESS SUCCESS SUCCESS	Desired Access: Query Value Type: REG_DWORD, Length: 4,	
1:17:48.6001722 PM calc.exe 1:17:48.6011060 PM calc.exe 1:17:48.6011278 PM calc.exe 1:17:48.6011278 PM calc.exe	2072 ReadFile 2072 CreateFile 2072 QueryBasicInfor 2072 CheeFile	C:Windows\System32\calc.exe C:Windows\System32\WindowsCodecs.dll C:Windows\System32\WindowsCodecs.dll C:Windows\System32\WindowsCodecs.dll	SUCCESS SUCCESS SUCCESS	Offset: 103,424, Length: 32,768, I Desired Access: Read Attributes, CreationTime: 7/13/2009 4:29:14	
1:17:48.6012132 PM calc.exe 1:17:48.6012342 PM calc.exe 1:17:48.6012344 PM calc.exe 1:17:48.6012901 PM calc.exe	2072 Create File 2072 Create File 2072 Create File Mapp 2072 Create File Mapp	C: Windows (System)22 (WindowsCodecs.dll C: Windows (System)22 (WindowsCodecs.dll C: Windows (System)22 (WindowsCodecs.dll C: Windows (System)22 (WindowsCodecs.dll C) Windows (System)22 (WindowsCodecs.dll)	SUCCESS FILE LOCKED WI SUCCESS	Desired Access: Read Data/List SyncType: SyncTypeCreateSecti SyncType: SyncTypeOther	
1:17:48.6013372 PM Calc.exe 1:17:48.60133796 PM Calc.exe 1:17:48.6015378 PM Calc.exe 1:17:48.6015591 PM Calc.exe	2072 Close File 2072 Close File 2072 RegOpen Key 2072 RegQuery Key	C:\Windows\System32\WindowsCodecs.all C:\Windows\System32\WindowsCodecs.dll HKCU\Software\Classes HKCU\Software\Classes	SUCCESS SUCCESS SUCCESS SUCCESS	Desired Access: Maximum Allowe Query: Name	
1:17:48.6015697 PM calc.exe 1:17:48.6015797 PM calc.exe 1:17:48.60150937 PM calc.exe 1:17:48.6016002 PM calc.exe 1:17:48.6016002 PM calc.exe	2072 RegOpenKey 2072 RegOpenKey 2072 RegQueryKey 2072 RegOpenKey 2072 RegOpenKey	HKCU/Software/Classes/CLSID/{FAE3D380-FEA4-4 HKCR/CLSID/{FAE3D380-FEA4-4623-8C75-C6B6111. HKCU/Software/Classes HKCU/Software/Classes/CLSID/{FAE3D380-FEA4-4	NAME NOT FOUND SUCCESS SUCCESS NAME NOT FOUND	Desired Access: Read Desired Access: Read Query: Name Desired Access: Read	
Showing 128,723 of 253,268 events (50%)	Backed by virtual	I memory		Desired Access; head	▼ 

#### **Process Monitor Toolbar**



### **Filtering with Exclude**

- One technique: hide normal activity before launching malware
- Right-click each Process Name and click **Exclude**
- Doesn't seem to work well with these samples

### **Filtering with Include**

Most useful filters: Process Name, Operation, and Detail

Display entries match Process Name	ing these condition	s: calc.exe	✓ then Include
Reset		_	Add Remove
Column	Relation	Value	Action
V 😵 Process N	is	Procmon.exe	Exclude
V 🐼 Process N	is	System	Exclude
🔽 🔕 Operation	begins with	IRP_MJ_	Exclude
🔽 🔕 Operation	begins with	FASTIO_	Exclude
🔽 🔕 Result	begins with	FAST IO	Exclude
🔽 🐼 Path	ends with	nagefile svs	Exclude
		ОК	Cancel Apply

### VIEWING PROCESSES WITH PROCESS EXPLORER

0.

### **Viewing Processes with Process Explorer**

- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

😂 Process Explorer - Sysinternals: w	ww.sysin	ternals.co	om [W7\studer	nt]			x
File Options View Process Fin	nd Use	rs Help	)				
🛃 🙆 🚍 🗉 🧮 🚱	Х М	•					
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name	^
System Idle Process	0	96.81	0 K	24 K			
🖃 🔝 System	4	0.09	48 K	560 K			
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	3	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation	=
CSrss.exe	348	< 0.01	1,252 K	3,164 K	Client Server Runtime Process	Microsoft Corporation	
🖃 🔳 wininit.exe	400		892 K	3,084 K	Windows Start-Up Application	Microsoft Corporation	
services.exe	504	0.01	3,972 K	6,640 K	Services and Controller app	Microsoft Corporation	
svchost.exe	652		2,700 K	6,024 K	Host Process for Windows S	Microsoft Corporation	
dllhost.exe	1716		6,176 K	4,804 K	COM Surrogate	Microsoft Corporation	
WmiPrvSE.exe	740		1,804 K	4,736 K	WMI Provider Host	Microsoft Corporation	
svchost.exe	724	< 0.01	2,972 K	6,012 K	Host Process for Windows S	. Microsoft Corporation	
svchost.exe	772		13,776 K	11,760 K	Host Process for Windows S	. Microsoft Corporation	
audiodg.exe	3200		14,960 K	13,972 K	Windows Audio Device Grap	. Microsoft Corporation	
svchost.exe	912		37,940 K	42,292 K	Host Process for Windows S	. Microsoft Corporation	
dwm.exe	3248	0.74	61,892 K	27,976 K	Desktop Window Manager	Microsoft Corporation	
svchost.exe	936	0.02	20,836 K	29,900 K	Host Process for Windows S	. Microsoft Corporation	
svchost.exe	1116	0.03	5,136 K	8,340 K	Host Process for Windows S	. Microsoft Corporation	
svchost.exe	1260	0.06	10,840 K	11,960 K	Host Process for Windows S	. Microsoft Corporation	
spoolsv.exe	1352		5,392 K	7,436 K	Spooler SubSystem App	Microsoft Corporation	
svchost.exe	1388		6,752 K	8,720 K	Host Process for Windows S	. Microsoft Corporation	
svchost.exe	1500		2,472 K	4,712 K	Host Process for Windows S	. Microsoft Corporation	
6 gogoc.exe	1592	< 0.01	1,216 K	3,920 K	gogoCLIENT	gogo6, Inc.	
vm vmtoolsd.exe	1728	0.07	7,260 K	10,368 K	VMware Tools Core Service	VMware, Inc.	-
svchost.exe	•						- F
CPU Usage: 3.19% Commit Charge	: 21.92%	Process	ses: 57 Physic	al Usage: 30.24	%		

#### **DLL Mode**

2 Process Expl	orer -	Sysinternals: www.sysinternals.co	m [W7\student]	
File Options	View	Process Find <u>D</u> LL <u>U</u> sers	<u>H</u> elp	
		System Information	Ctrl+I	
Process		Show Process Tree	Ctrl+T	Set Description Company Name  A K Windows Company Research Company in
□ □ □ chrome	$\checkmark$	Show Processes From All Users		2 K Google Chrome Google Inc.
Chro	$\checkmark$	Show Fractional CPU		0 K Google Chrome Google Inc.
		Format I/O Bytes Columns		8 K Google Chrome Google Inc.
		Scroll to New Processes		0 K Notepad Microsoft Corporation
🗆 😂 soffice.exe		Show Unnamed Handles and Ma	ppings	4 K OpenOffice.org 3.4.1 OpenOffice.org
soffice.				4 K OpenOffice.org 3.4.1 OpenOffice.org
		Opacity	•	
Name	$\checkmark$	Show Lower Pane	Ctrl+L	Path
advapi32.dll		Lower Pane View	•	✓ DLLs Ctrl+D 2.dll
apisetschema.dll chrome.dll		Refresh Now	F5	Handles Ctrl+H al\Google\Chrome\Applicati
chrome.exe chrome_100_perc		Update Speed	•	C:\Users\student\AppData\Local\Google\Chrome\Applicati C:\Users\student\AppData\Local\Google\Chrome\Applicati
comctl32.dll crypt32.dll		Organize Column Sets		C:\Windows\winxxs\x86_microsoft.windows.common-contro C:\Windows\System32\crypt32.dll
cryptbase.dll		Save Column Set		C:\Windows\System32\cryptbase.dll
dbghelp.dll en-US.pak		Load Column Set	+	C:\Windows\System32\dbghelp.dll C:\Users\student\AppData\Local\Google\Chrome\Applicati
ffmpegsumo.dll gdi32.dll		Select Columns		C:\Users\student\AppData\Local\Google\Chrome\Applicati C:\Windows\System32\gdi32.dll
icudt.dll		CU Data DLL	The ICU Project	C:\Users\student\AppData\Local\Google\Chrome\Applicati
imm32.dll	I.	Multi-User Windows IMM32 API Cli 1	Microsoft Corporation	C:\Windows\System32\imm32.dll
Kemel32.dll		Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kemel32.dll
libpeerconnection	dli 0	Soogle Chrome (	Google Inc.	C:\Users\student\AppData\Local\Google\Chrome\Applicati
CPU Usage: 4.58	%	Commit Charge: 21.56% Proces	ses: 53 Physical Usag	e: 30.02%

### **Properties**

- Shows DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization) status
- Verify button checks the disk file's Windows signature

   But not the RAM image, so it won't detect process replacement



### Strings

Compare **Image** to **Memory** strings, if they are very different, it can indicate process replacement

### **Detecting Malicious Documents**

- Open the document (e.g. PDF) on a system with a vulnerable application
- Watch Process Explorer to see if it launches a process
- The Image tab of that process's Properties sheet will show where the malware is

COMPARING REGISTRY SNAPSHOTS WITH REGSHOT

### Regshot

- Take 1st shot
- Run malware
- Take 2nd shot
- Compare them to see what registry keys were changed

💑 Regshot 1.8.3-beta1V5	- • ×
Compare logs save as:	1st shot 2nd shot
Scan dir 1[;dir2;dir3;;dir nn]: C:\Windows	Compare
Output path: C:\Users\student\AppData\	Quit About
Add comment into the log:	English 🔻

# FAKING A NETWORK

•

•

### **ApateDNS**

- Spoofing DNS responses to a user-specified IP address
- Listening on UDP port 53 on the local machine
- Responding to DNS requests using a predefined IP address

ApateDNS			_ 🗆 🗙
Capture Windo	ow DNS Hex View		
Time 13:22:08	Domain Requested evil.malwar3.com	DNS Returned FOUND	
[+] Using 127. [+] DNS set to [+] Sending va [+] Server start	0.0.1 as return DNS IP! 127.0.0.1 on AMD PCNET Family PCI Ethemet Adapter - Packet Sche alid DNS response of first request. ted at 13:21:26 successfully.	eduler Miniport.	
DNS Rep # of NXD Selected	Ny IP (Default: Current Gatway/DNS): 127.0.0.1 OMAIN's: Interface: AMD PCNET Family PCI Ether	Start Se Net Adapter - P	erver erver

### **Ncat Listener**

- Using Ncat.exe, you can listen on a single TCP port in Windows
  - In Linux, use nc (netcat)
- This will allow malware to complete a TCP handshake, so you get some rudimentary information about its requests
- But it's not a real server, so it won't reply to requests after the handshake

## Monitoring with Ncat (included with Nmap)

📷 Administrator: cmd - Shortcut (2) - ncat -I 80	
C:\Windows\System32>ncat -1 80 GET / HTTP/1.1 Host: 127.0.0.1 Connection: keep-alive Accept: text/html.application/xhtml+xml.application/xml;q=0.9 User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 Safari/537.36 Accept-Encoding: gzip.deflate,sdch Accept-Language: en-US,en;q=0.8	,*/*;q=0.8 .KHTML, like Gecko> Chrome/29.0.1547.57
	C:\> nc -1 -p 80 <b>0</b>
	POST /cq/frame.htm HTTP/1.1
	Host: www.google.com 🛛
	User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWFsd2FyZUh1bnRlcg==;
	rv:1.38)
	Accept: text/html, application
http://qwe.net/ is not avai ×	Accept-Language: en-US, en:q=
← → × ♠ 🗋 127.0.0.1 🎲 🚍	Accept-Encoding: gzip, deflate
🙉 samsclass.info: Sam 🍞 virustotal - Google S 🕒 L	Keep-Alive: 300
	Content-Type: application/x-form-urlencoded
	Content-Length
	Microsoft Windows XP [Version 5.1.2600]
This webpage is not available	(C) Copyright 1985-2001 Microsott Corp.
Waiting for 127.0.0.1	
	Z:\Maiware> 😝

### **Packet Sniffing with Wireshark**

🗖 Ca	pturing	g fror	n Int	el(R)	PRC	0/100	00 M	T Net	work	Conr	nect	ion										_ 0	23	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	v <u>G</u>	0	<u>C</u> apt	ure	<u>A</u> na	alyze	<u>S</u> tat	istics	Т	elep	hony	<u>(</u> I	ools	Inter	nals	<u>H</u> elp						
		í 🔒	( 🗎			8	X	2	₽	C	6	¢a	•		7	₽		T.	€ (	<b>)</b> (1)	( 🖭			»>
Filter	: http															-	Express	ion	Clear	App	y			
No.	Tim	ie			Sour	ce				Des	tina	ntion				Proto	col 1	Info				_		*
11(	DE 7.	5373	236		192	1.81	0	31	L 54	10	2 1	1.68	110	ן 1 ב	54	HII	D	GET,	/ <b>T.</b> g /1 1	200	=1377	(PNG)	1001	
11(	08 7.	5574	449		93.	184	. 21	6.1	39	19	2.1	168	.11	9.1	54	HTT	P	ГТСР	Ret	ransr	nissi	ion] c	onti	
111	LO 7.	5902	291		23.	65.	1.2	24		19	2.1	168	.119	9.1	54	HTT	Р	нттр,	/1.1	200	OK	(GIF8	9a)	
111	L1 7.	6912	258		23.	65.	1.2	24		19	2.1	168	.119	9.1	54	HTT	Р	[TCP	Ret	ransı	nissi	ion]⊦	ITTP/	
118	39 36	. 858	8744	4	192	.16	8.1	19.1	L54	19	9.1	16.3	156.	. 21		HTT	Р	GET ,	/wid	gets,	/time	elines	/pag	
119	93 36	. 88	1799	9	192	.16	8.1	19.1	L54	19	9.1	16.	156	. 21		HTT	P	GET ,	/wid	gets/	time	elines	/pac	
110	90 30 30 27	. 954	4204	+ >	199	1.10	.15	6.2	L 1	10	2.1	168	110	9.13	54 54	HII	P D	нттр,	/1.1 /1 1	200	OK	(app)	icat	
13/	50 06	. 04:	0725	5	199	16	. 1 ) R 1	10.2	54	10	2.J 0.1	16	156	9.1: 21	54	HTT	P	GET	/uid	200	UK /time	lines	/nac	
137	73 96	.772	2892	2	192	2.16	8.1	19.1	154	19	9.1	16.3	156.	. 21		нтт	Р	GET	/wid	aets/	/time	lines	/pag	
137	76 96	. 840	6439	9	199	).16	.15	6.21	L	19	2.1	168	.119	9.1	54	HTT	Р	нттр,	/1.1	200	OK	(app]	icat	Ξ
138	31 96	. 944	4497	7	199	.16	.15	6.21	L	19	2.1	168	.119	9.1	54	HTT	Р	нттр,	/1.1	200	ок	(app]	icat	Ŧ
۰																							P.	
	ame	48:	437	7 b	yte:	s oi	n w	ire	(349	96 b	it	s),	43	7 b'	yte	s cap	oture	d (34	196 l	oits)				*
	hern	et 1	II,	Sr	: ۱	Vmwa	are_	_52:	34:9	92 (	00	:0c	:29	:52	: 34	:92)	Dst	: Vmv	vare_	_e3:2	2:f1	(00:	50:5	
🕀 Ir	ntern	et F	Prot	toc	יוס	ver:	sio	n 4,	Sno	:: 1	.92	.16	8.1	19.	154	(192	2.168	.119.	154	), Ds	it: 1	.41.10	1.11	-
-				_	_	_	_		1	11			_	_	_								+	_
0000	00	50	56	e3	22	f1	00	0c	29	52	34	92	08	00	45	00	. PV.	"···	)R4	E	•	C	_	-
0010	75	a/ 98	05	25 a9	40	50	80 0c	80	cd	00 2e	dc	að ff	73	9a 93	80 50	18		6a		. W	e		_	
0030	fa	fŏ	Зc	da	00	õõ	47	45	54	20	2f	20	48	54	54	50	<	GE	т/	нтт	P		🖳 sa	ms
0040	2f	31	2e	31	0d	0a	48	6f	73	74 6f	3a	20	73	61 6f	6d	73	/1.1	L. Ho	st:	sam	s			2
0060	65	63	74	69	6f	6e	3a	20	6b	65	65	70	2d	61	6c	69	ect	ion:	kee	p-al	i			1
0070	76	65	0d	0a	41	63	63	65	70	74	3a	20	74	65	78	74	ve.	Acce	pt:	tex	t	8	🔒 sam	nscl
0080	2T 6e	68 2f	74 78	68	6C 74	2C 6d	01 6C	2b	70	oc 6d	69 6c	63 20	61 61	/4 70	69 70	от 6с	/ntr	ni,ap html+	y pin xml	cati .app	1			25
00a0	69	63	61	74	69	6f	6e	2f	78	6d	6c	3b	71	3d	30	2e	icat	ion/	xml	: a=0				
🔵 In	tel(R) P	RO/1	1000	MT	Netw	/ork (	Conn	nectio	n: <li< td=""><td>ve ca</td><td>ptu</td><td>re in</td><td>pro</td><td>. P</td><td>acke</td><td>ts: 139</td><td>8 Dis</td><td>Prof</td><td>ile: De</td><td>fault</td><td></td><td></td><td></td><td></td></li<>	ve ca	ptu	re in	pro	. P	acke	ts: 139	8 Dis	Prof	ile: De	fault				

## **Follow TCP Stream**

 Can save files from streams here too



### **USING INETSIM**

### **INetSim**

- Included in Kali Linux
- Simulates the Internet, including

   HTTP / HTTPS
  - $\circ\,$  SMTP, POP3
  - o DNS
  - $\circ$  FTP
  - $\circ$  Much more

### **INetSim**

kali-linux-i386-gnome-vm	O         O         Windows 7-Attacker-P@ssw0rd123
ons Places ổ 📃 🛛 Sun Aug 25, 3:57 PM 🛛 😭 🔍 🚅 🗬 root	Internet Protocol Version 4 (TCP/IPv4) Properties
root@kali: /etc/default Output: Muted ×	General Alternate Configuration
View Search Terminal Help	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Link encap:Ethernet HWaddr 00:0c:29:bf:b0:5a	Obtain an IP address automatically
inet addr:192.168.1.132	O Use the following IP address:
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1	IP address:
TX packets:15764 errors:0 dropped:0 overruns:0 carrier:0	Subnet mask:
collisions:0 txqueuelen:1000 BX bytos:29371297 (28 0 MiB) _ TX bytos:1152819 (1 0 MiB)	Default gateway:
Interrupt:19 Base address:0x2024	Obtain DNS server address automatically
i:/etc/default#	Use the following DNS server addresses:
	Preferred DNS server: 192 . 168 . 1 . 132
	Alternate DNS server:
	Validate settings upon exit Advanced
	OK Cancel

#### **INetSim Fools a Browser**

SIM INetSim default HTML pag ×
← → C ♠ 🗋 fred.com 😒 ≡
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.

### **INetSim Fools Nmap**

scan Tools Flottie Helb	
Target:     fred.com     Profile:     Intense scan     Scan     Cancel	
Command: nmap -T4 -A -v fred.com	
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans	
OS 4 Host nmap -T4 -A -v fred.com	
<pre>fred.com (192.168.1 Starting Nmap 5.61TEST5 ( http://nmap.org ) at 2013-08-25 12:52 Pacific Daylight Time NSE: Loaded 92 scripts for scanning. NSE: Script Pre-scanning. Initiating ARP Ping Scan at 12:52 Scanning fred.com (192.168.1.132) [1 port] Completed ARP Ping Scan at 12:52, 0.07s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 12:52 Completed Parallel DNS resolution of 1 host. at 12:52 Scanning fred.com (192.168.1.132) [1000 ports] Discovered open port 21/tcp on 192.168.1.132 Discovered open port 80/tcp on 192.168.1.132 Discovered open port 43/tcp on 192.168.1.132 Discovered open port 25/tcp on 192.168.1.132 Discovered open port 110/tcp on 192.168.1.132 Discovered open port 110/tcp on 192.168.1.132 Discovered open port 95/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 110/tcp on 192.168.1.132 Discovered open port 110/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 110/tcp on 192.168.1.132 Discovered open port 113/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 90/tcp on 192.168.1.132 Discovered open port 91/tcp on 192.168.</pre>	
Ulscovered open port 7/tcp on 192.168.1.132     Completed SVN Stealth Scan at 12:52, 0.11s elapsed (1000     tots reach)	
Filter Hosts	

## BASIC DYNAMIC TOOLS IN PRACTICE

0

0.

### Using the Tools

Procmon

 Filter on the malware executable name and clear all events just before running it

- Process Explorer
- Regshot
- Virtual Network with INetSim
- Wireshark

### **Example of a Virtual Network**



#### Examining the malware *msts.exe*

 Examine <u>ApateDNS</u> to see if DNS requests were performed

l	M ApateDNS							
1	Capture Wi	ndow	DNS Hex View					
	Time	Doma	in Requested	DNS Returned				
	14:20:24	www.	malwareanalysisbook.com	FOUND				

• Review the **Procmon** results for file system modifications

Process Monitor - Sysinternals: www.sysinternals.com									
File Edit	Event	Filter Tools Op	ptions	Help					
🖻 🖬	<b>\$</b>	🗈 🗠   🗢	<u>A</u>	🕀   🏘	ろ 🛛 戱 🗟 🖓 🗷				
Sequence	Time	Process Name	PID	Operation	Path	Result	Detail		
141	4:55:	msts.exe	1800	CreateFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Desired Access: Generic Write		
142	4:55:	msts.exe	1800	WriteFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Offset: 0, Length: 7,168		
143	4:55:	msts.exe	1800	CloseFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	•		

Compare the two snapshots taken with <u>Regshot</u> to identify changes

Values added:3

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\winhlp: C:\WINDOWS\system32\winhlp2.exe

 Use <u>Process Explorer</u> to examine the process to determine whether it creates **mutexes** or listens for incoming connections

File       Options       View       Process       Find       Handle       Users       Help         Process       PID       CPU       Description       Company Name         Svchost.exe       980       Generic Host Process fo       Microsoft Corporation         Svchost.exe       1024       Generic Host Process fo       Microsoft Corporation         Svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         Svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         Svchost.exe       1292       Spooler Sub System App       Microsoft Corporation         Spoolsv.exe       1292       Spooler Sub System App       Microsoft Corporation         PortReport       1428       Application Layer Gate       Microsoft Corporation         Blass.exe       1512       VMware Tools Service       VMware, Inc.         Spolorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         WMwareTray.exe       168       Application Layer Gate       Microsoft Corporation         WMwareTray.exe       176       VMware Tools Service       VMware, Inc.         WirdwareTray.exe       176       VMware Tools Service       VMware, Inc.	Process Explorer - Sysinternals: www.sysinternals.com [MALWAREHUNTER\user]							
Process       PID       CPU       Description       Company Name         ■ svchost.exe       980       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1024       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ sychost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ spoolsv.exe       1292       Spooler SubSystem App       Microsoft Corporation         ■ PortReport       1428       Microsoft Corporation         ■ portReport       1428       Microsoft Corporation         ■ spoolsv.exe       1512       VMware Tools Service       VMware, Inc.         ■ alg.exe       1512       VMware Tools Service       Microsoft Corporation         ■ sass.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ■ worker Tray.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ■ procexp.exe       1892       Sysintern	File Options View Pr	ile Options View Process Find Handle Users Help						
Process       PID       CPU       Description       Company Name         ■ svchost.exe       980       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1024       Generic Host Process fo       Microsoft Corporation         ■ wschty       204       Windows Security Cent       Microsoft Corporation         ■ wschost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ sychost.exe       1292       Spooler Sub System App       Microsoft Corporation         ■ spoolsv.exe       1292       Spooler Sub System App       Microsoft Corporation         ■ portReport       1428        VMware Tools Service       VMware, Inc.         ■ alg.exe       1688       Application Layer Gate       Microsoft Corporation         ■ spooler.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ● VMwareUser.exe       176       VMware Tools Service       VMware, Inc.         ● procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ● procexp.exe       1992       Sysinternals Process Ex       Sysinternals <td< th=""><th></th><th>II 🔊 🖻 🖞</th><th>* #</th><th></th><th>Maria</th><th></th></td<>		II 🔊 🖻 🖞	* #		Maria			
■ svchost.exe       980       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1024       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1292       Spooler Sub System App       Microsoft Corporation         ■ portReport       1428       1428       Microsoft Corporation         ■ optrReport       1428       1512       VMware Tools Service       VMware, Inc.         ■ alg.exe       168       Application Layer Gate       Microsoft Corporation         ■ explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ■ explorer.exe       196       1.54       Windows Explorer       Microsoft Corporation         ■ procexp.exe       1992       Sysinternals Process Ex       Sysinternals <td>Process</td> <td></td> <td>PID</td> <td>CPU</td> <td>Description</td> <td>Company Name</td>	Process		PID	CPU	Description	Company Name		
□ svchost.exe       1024       Generic Host Process fo       Microsoft Corporation         □ wscntfy       204       Windows Security Cent       Microsoft Corporation         □ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         □ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         □ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         □ spoolsv.exe       1292       Spooler Sub System App       Microsoft Corporation         □ PortReport       1428         □ VMware Se       1512       VMware Tools Service       VMware, Inc.         □ alg.exe       1688       Application Layer Gate       Microsoft Corporation         □ sass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         □ explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □ explorer.exe       196       1.54       Windows Explorer       Microsoft Corporation         □ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         □ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         □ msts.exe       1152       Itse	sv	/chost.exe	980		Generic Host Process fo	Microsoft Corporation		
□wscntfy       204       Windows Security Cent       Microsoft Corporation         □svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         □svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         □spoolsv.exe       1292       Spooler SubSystem App       Microsoft Corporation         □PortReport       1428         □VMware Se       1512       VMware Tools Service       VMware, Inc.         □alg.exe       1688       Application Layer Gate       Microsoft Corporation         □spoolsv.exe       196       1.54       Windows Explorer       Microsoft Corporation         □system Process.exe       1428       VMware Tools Service       VMware, Inc.         □yMwareUser.exe       168       VMware Tools Service       VMware, Inc.         □yVMwareUser.exe       176       VMware Tools Service       VMware, Inc.         □yorcexp.exe       1992       Sysinternals Process Ex       Sysinternals         □type ▲       Name       Name       Interviews State       Key         Key       HKLM\SYSTEM\Control Set001\Services\Tcpip\Parameters       Key       Key         HKLM\SYSTEM\Control Set001\Services\NetBT\Parameters       KeyetEvent       KernelObjects\CritSecOutOfMe	🖃 🔤 sv	/chost.exe	1024		Generic Host Process fo	Microsoft Corporation		
■ svchost.exe       1076       Generic Host Process fo       Microsoft Corporation         ■ svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■ spoolsv.exe       1292       Spooler Sub System App       Microsoft Corporation         ■ PortReport       1428         ● VMware Se       1512       VMware Tools Service       VMware, Inc.         ■ alg.exe       1688       Application Layer Gate       Microsoft Corporation         ■ lsass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         ■ sexplorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ● explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ● procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ■ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ■ mst.exe       1152       Itse       Microsoft Corporation         ■ first.exe       1152       Itse       Microsoft Corporation         ■ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ■ mst.exe       1152       Itse       Microsoft Corporation		wscntfy	204		Windows Security Cent	Microsoft Corporation		
■svchost.exe       1188       Generic Host Process fo       Microsoft Corporation         ■spoolsv.exe       1292       Spooler SubSystem App       Microsoft Corporation         ■PortReport       1428         ●VMware Se       1512       VMware Tools Service       VMware, Inc.         ■alg.exe       1688       Application Layer Gate       Microsoft Corporation         ■Isass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         ■sexplorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ●vMwareTray.exe       168       VMware Tools Service       VMware, Inc.         ● procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ● procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ● Type ▲       Name       ItS2       ItSevices\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters       KeyetEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1       Thread       msts.exe(1152): 1260       MindowStations\Window Stations\WinSta0         WindowStati       Windows\WindowStations\WinSta0       WindowStations\WinSta0       WindowStations\WinSta0	sv	chost.exe	1076		Generic Host Process fo	Microsoft Corporation		
□spoolsv.exe       1292       Spooler Sub System App       Microsoft Corporation         □PortReport       1428         □VMware Se       1512       VMware Tools Service       VMware, Inc.         □alg.exe       1688       Application Layer Gate       Microsoft Corporation         □lsass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         □system Tray.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □VMwareTray.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □YMwareTray.exe       168       VMware Tools Service       VMware, Inc.         □YMwareUser.exe       176       VMware Tools Service       VMware, Inc.         □Yprocexp.exe       1992       Sysinternals Process Ex       Sysinternals         □rsts.exe       1152         Type       Name         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeydEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260	= sv	/chost.exe	1188		Generic Host Process fo	Microsoft Corporation		
□PortReport       1428         □VMware Se       1512       VMware Tools Service       VMware, Inc.         □alg.exe       1688       Application Layer Gate       Microsoft Corporation         □Isass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         □Port.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □VMwareTray.exe       168       VMware Tools tray appli       VMware, Inc.         □VMwareUser.exe       176       VMware Tools Service       VMware, Inc.         □procexp.exe       1992       Sysinternals Process Ex       Sysinternals         □msts.exe       1152	i sp	oolsv.exe	1292		Spooler SubSystem App	Microsoft Corporation		
Image: Service       VMware Se         Image: Service       VMware, Inc.         Image: Service       VMware, Inc.         Image: Service       Isses.exe         Image: Service Service       Isses.exe         Image: Service Service       Isses.exe         Image: Service Service       Isses.exe         Image: Service Service Service       Isses.exe         Image: Service Service Service Service Service       Isses         Image: Service		ortReport	1428					
□ alg.exe       1688       Application Layer Gate       Microsoft Corporation         □ lsass.exe       740       LSA Shell (Export Versi       Microsoft Corporation         □ explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □ VMwareTray.exe       168       VMware Tools tray appli       VMware, Inc.         □ VMwareUser.exe       176       VMware Tools Service       VMware, Inc.         □ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         □ msts.exe       1152         Type ▲       Name         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Levi1         Thread       msts.exe(1152): 1260         WindowStati       WindowStations\WinSta0         WindowStati       WindowStations\WinSta0	∎v	Mware Se	1512		VMware Tools Service	VMware, Inc.		
Isass.exe       740       LSA Shell (Export Versi Microsoft Corporation         ■ explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         ■ VMwareTray.exe       168       VMware Tools tray appli       VMware, Inc.         ■ VMwareUser.exe       176       VMware Tools Service       VMware, Inc.         ■ procexp.exe       1992       Sysinternals Process Ex       Sysinternals         ■ Type       Name       1152         Type       Name       Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Levil1         Thread       msts.exe(1152): 1260         WindowStati       Windows\UndowStations\WinSta0         WindowStati       Windows\UndowStations\WinSta0	al	lg.exe	1688		Application Layer Gate	Microsoft Corporation		
□       explorer.exe       1896       1.54       Windows Explorer       Microsoft Corporation         □       WMwareTray.exe       168       VMware Tools tray appli       VMware, Inc.         □       Procexp.exe       176       VMware Tools Service       VMware, Inc.         □       Procexp.exe       1992       Sysinternals Process Ex       Sysinternals         □       msts.exe       1152         □       Type ▲       Name       Implementation         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Levil1         Thread       msts.exe(1152): 1260         WindowStati       WindowStations\WinSta0         WindowStati       Windows\WindowStations\WinSta0	Isass	s.exe	740		LSA Shell (Export Versi Mi	Microsoft Corporation		
Image: Second Strain Strai	🗆 🕃 explorer.exe		1896 1	1.54	Windows Explorer	Microsoft Corporation		
Image: Systematic Service       VMware User.exe         Image: Systematic Service       VMware, Inc.         Image: Systematic Service       1992         Systematic Service       Systematic Service         Image: Systematic Service Service       Systematic Service         Image: Systematic Service	WMwareTray	y.exe	168		VMware Tools tray appli	VMware, Inc.		
Image: Process exe       1992       Sysinternals Process Ex Sysinternals         Imsts.exe       1152         Type A       Name         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeydEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260         WindowStati       \Windows\Window Stations\WinSta0         WindowStati       \Windows\Window Stations\WinSta0	🔁 VMwareUse	r.exe	176		VMware Tools Service	VMware, Inc.		
Type       Name         Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeydEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260         WindowStati       \Windowstations\WinSta0         WindowStati       \Windowstations\WinSta0	🖉 procexp.exe	e '	1992		Sysinternals Process Ex	Sysinternals		
Type         Name           Key         HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters           KeyedEvent         \KernelObjects\CritSecOutOfMemoryEvent           Mutant         \BaseNamedObjects\Evil1           Thread         msts.exe(1152): 1260           WindowStati         \Windowstations\WinSta0           WindowStati         \Windows\Window Stations\WinSta0	msts.exe		1152					
Type         Name           Key         HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters           Key         HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters           Mutant         \BaseNamedObjects\CritSecOutOfMemoryEvent           Mutant         \BaseNamedObjects\CritSecOutOfMemoryEvent           Mutant         \BaseNamedObjects\CritSecOutOfMemoryEvent           Mutant         \BaseNamedObjects\CritSecOutOfMemoryEvent           Window         Mutant           \BaseNamedObjects\CritSecOutOfMemoryEvent           WindowStati         \WindowsYuindowStations\WinSta0           WindowStati         \WindowsWindowStations\WinSta0								
Key       HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260         WindowStati       \Windows\UndowStations\WinSta0         WindowStati       \Windows\UndowStations\WinSta0	Type 🛆 🛛 Nai	me						
Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces         Key       HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters         KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260         WindowStati       \Windows\tations\WinSta0         WindowStati       \Windows\tations\WinSta0	Key HKL	.M\SYSTEM\0	\ControlSet001\Services\Tcpip\Parameters					
Key     HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters       KeyedEvent     \KernelObjects\CritSecOutOfMemoryEvent       Mutant     \BaseNamedObjects\Evil1       Thread     msts.exe(1152): 1260       WindowStati     \WindowStations\WinSta0       WindowStati     \WindowStations\WinSta0	Key HKL	HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces						
KeyedEvent       \KernelObjects\CritSecOutOfMemoryEvent         Mutant       \BaseNamedObjects\Evil1         Thread       msts.exe(1152): 1260         Thread       msts.exe(1152): 1260         WindowStati       \Windows\WindowStations\WinSta0         WindowStati       \Windows\WindowStations\WinSta0	Key HKL	HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters						
Mutant         \BaseNamedObjects\Evil1           Thread         msts.exe(1152): 1260           Thread         msts.exe(1152): 1260           WindowStati         \WindowS\WindowStations\WinSta0           WindowStati         \WindowS\WindowStations\WinSta0	KeyedEvent \Ker	\KernelObjects\CritSecOutOfMemoryEvent						
Thread msts.exe(1152): 1260 Thread msts.exe(1152): 1260 WindowStati \Windows\WindowStations\WinSta0 WindowStati \Windows\WindowStations\WinSta0	Mutant \Bas	\BaseNamedObjects\Evil1						
Thread msts.exe(1152): 1260 WindowStati \Windows\WindowStations\WinSta0 WindowStati \Windows\WindowStations\WinSta0	Thread mst	msts.exe(1152): 1260						
WindowStati \Windows\WindowStations\WinSta0 WindowStati \Windows\WindowStations\WinSta0	Thread mst	msts.exe(1152): 1260						
Window Stati \Windows\Window Stations\WinSta0	WindowStati \Win	\Windows\WindowStations\WinSta0						
	WindowStati \Win	/indowStati \Windows\WindowStations\WinSta0						
			4 2024	-				

Review the <u>INetSim</u> logs for requests and attempted connections on standard services

[2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043] connect [2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043] Error setting up SSL: SSL accept attempt failed with unknown error Error:140760FC:SSL routines:SSL23\_GET\_CLIENT\_HELL0:unknown protocol [2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043] disconnect

Review the <u>Wireshark</u> capture for network traffic generated by the malware

Tollow TCP Stream	
Stream Content	
Ib00<.0.]#94 w];b,Q.h#.s\"Qy∪(.k .j.S*U6v5.wbZ345.	[s27KD^I>\+.A[4ce.].
Eind Save As Print Entire conversation (256 bytes)	SASCII O EBCDIC O Hex Dump O C Arrays O Raw
Help	<u>C</u> lose Filter Out This Stream



# END OF LECTURE. THANK YOU.