

Malicious Code Analysis

Fangtian Zhong
CSCI 591

Gianforte School of Computing
Norm Asbjornson College of Engineering
E-mail: fangtian.zhong@montana.edu





Part One

01

2025-10-19

Dynamic Malware Analysis

An isometric illustration of a digital workspace. It features several stylized figures: a person in a suit standing near a large screen displaying a grid, a person in a light blue shirt walking, and a woman in a dark dress talking to a man in a white shirt. The background is filled with floating rectangular panels, some showing star ratings, and a large padlock icon on the right. The overall color scheme is light blue and white, with a red vertical bar on the left side of the slide.



What is Dynamic Analysis?

☐ Allow the malware to run.



☐ Complement static analysis.

☐ Help us to understand the program behavior.



Dynamic Analysis

Basic dynamic analysis

- Executing target binary and observing its behavior.

Advanced dynamic analysis

- Executing target binary and using a debugger to analyze internal states.



Basic Dynamic Analysis

- Monitored execution of a program in order to perform analysis.
- Often performed after static analysis is done.

Advantages

- Efficient way to determine program functionality.
- Able to check file activity, process creation, network activity, etc.

Disadvantages

- Non-functional paths may be explored.



Executing the Malware

 In most cases, you can just double-click the “exe” file.

➤ You may want to run it from the command-line as well.

 What if the extension is not “exe”?

➤ You can change it. Verify if it is a PE file using a PE parser.

 What if it is a DLL?

➤ You can run a DLL using the rundll32 program.

➤ Format: C:\> rundll32.exe <name>.dll



Dynamic Analysis Systems



Dynamic analysis is run in a safe environment on dedicated physical or virtual machines (in order not to expose the users' system to unnecessary risks)

- **Physical machines** are set up on isolated networks, disconnected from the Internet or any other network, to prevent malware from spreading
- **Virtual machines** emulate the functionality of a physical computer, where the OS running on the virtual machine is isolated from the host OS
 - *One limitation is that some malware can detect when they are running in a virtual machine, and they will execute differently than when in a physical machine*
- A related term is **sandbox**, referring to a physical or virtual environment for running malware, which isolates executables from other system resources and applications.
 - *Although they share characteristics with physical and virtual machines, sandboxes can be more limited (e.g., they can run in the browser), while physical and virtual machines always act as a complete system*
 - *For example, online sandboxes are websites where one can submit a sample file and receive a report about its behavior*



Dynamic Features for Malware Classification

- 🏆 **Dynamic features** are extracted from the execution of malware at runtime
 - **Memory and registers usage** - values stored in the memory and different registers during the execution can distinguish benign from malicious programs
 - [Ghiasi et al. \(2015\)](#) monitored the memory content and register values before and after each invoked API call
 - They used similarity scores between the benign and malicious files in a training set to train an ML model for malware detection
 - **Instruction traces** - sequence of processor instructions called during the execution of a program
 - Dynamic instruction traces are more robust indicators of the program's behavior than static traces, since compression and encryption can obfuscate code instructions from static analysis
 - [Carlin et al. \(2017\)](#) analyzed traces of opcodes to detect malware by Random Forest and Hidden Markov Model classifiers



Dynamic Features for Malware Classification

- **Network traffic** - monitoring the traffic entering and exiting the network can provide helpful information to detect malicious behavior
 - E.g., when malware infects a host machine, it may establish communication with an external server to download updates, other malware, or leak private and sensitive information from the host machine
 - [Bekerman et al. \(2015\)](#) extracted 972 features from the network traffic, and used them for developing Decision Tree and Random Forest malware classifiers
- **API call traces** - traces for accessing file systems, devices, processes, threads and error handling, and also to access functions such as the Windows registry, manage user accounts, etc.
 - [Uppal et al. \(2014\)](#) proposed traditional ML-based classifiers using n-grams of features extracted from traces of invoked API calls.



Sandboxing

- ★ Sandboxing is a security technique used to isolate running applications from the rest of the system. It works by creating a virtual environment, or sandbox, in which an application or process can run without affecting other parts of the system.
- ★ The sandboxed environment provides a controlled and secure environment for testing or running potentially risky applications. If the application performs any suspicious behavior, it will be confined within the sandbox and prevented from affecting other parts of the system.



Sandboxing



Sandboxing can be implemented in various ways, such as virtual machines, containerization, or operating system-level sandboxes. For example, a virtual machine can be used to create a separate operating system environment within the host operating system, while containerization can be used to create isolated environments for individual applications or processes.



Sandboxes

- 💎 All-in-one software solutions to analyze the execution of a program.
- 💎 Provides security mechanisms for running untrusted programs in a safe environment.
- 💎 Lets you monitor behavior/changes to the system.
- 💎 The “real” system remains isolated-so, it does not get infected.





Sandboxes



Usually use virtual components

- Simulates network services to allow program to execute as it “normally” would



Sandboxes for malware analysis

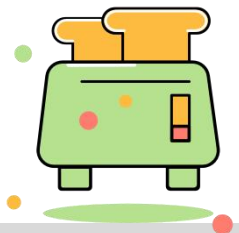
- There are many free and commercial versions available
- Lets you analyze a variety of file types: EXE, PDF, Office documents, URLs, etc.





Sandboxes-drawbacks

- ★ May run the EXE w/o command line arguments.
- ★ Execution may wait for response from C2.
- ★ Malware may find out that it is running in a sandbox .
 - an anti-analysis technique
 - in that case, the malware may change its behavior
- ★ Often the environment is not properly setup.





Sandbox-Example: <https://any.run/>

The screenshot displays the ANY.RUN website, which is a platform for analyzing malware in a secure, interactive sandbox environment. The website's header includes navigation links: INTERACTIVE MALWARE, WHY US, SERVICE, TRACKER, REPORTS, FEATURES, INTEGRATIONS, PRICING, BLOG, CONTACTS, MEDIA KIT, and DEMO. The main heading is "HEART OF AN INCIDENT", followed by a description: "Watch the epidemic as if it was on your computer, but in a more convenient and secure way, with a variety of monitoring features." A prominent green button labeled "LET'S HUNT!" is positioned below the text.

The central part of the image shows a simulated Windows desktop environment within the ANY.RUN browser window. The desktop features a taskbar with various application icons, including "New task", "Public tasks", "History", and "7.32 bit". A central window titled "Wanna Decryptor 2.0" displays a ransomware message: "Oops, your files have been encrypted!". The message includes instructions on how to recover files, a payment deadline of 02:23:54:09, and a Bitcoin payment address: 128YDPgwueZ3NyMgw5t9p7AA8isjr6SMw. The desktop also shows a "WannaCry.exe" process running, with a status bar indicating "Win7 32 bit Complete" and a timer set to 03:01. The "Tracker" section shows the CPU usage at 2% and RAM usage at 21%.

On the right side of the desktop, a "Processes" list is visible, showing the following running processes:

Process ID	Process Name	Architecture	Working Set	Private Bytes	Page Faults	Session ID	Process ID
1484	WannaCry.exe	PE	28k	18	125		
3116	attrib.exe	+h.	54	0	30		
4008	lscls.exe	./grant Everyone:F /T /C /Q	844	0	20		
3216	taskkill.exe	PE	21	0	12		
2984	cmd.exe	/c 277721601449320.bat	310	6	34		



Monitor System Activity



Process Monitor

- ☐ Allow monitoring of registry, file system, network, process, and thread activities.
- ☐ Monitor all system calls
- ☐ Captures a lot of data (>50,000 events in a minute)
- ☐ Use RAM to capture events
 - can easily crash a VM - so, run for a limited amount of time
- ☐ Not a reliable tool for network activities
 - so other tools needs to be used



The image shows a Windows 'Event Properties' window with the 'Process' tab selected. It displays details for the process 'svchost.exe' (Host Process for Windows Services) running as 'NT AUTHORITY\SYSTEM'. The command line is 'C:\WINDOWS\system32\svchost.exe -k appmodel -p -s StateRepository'. Below this, a 'Modules' table lists loaded DLLs. At the bottom, there are buttons for 'Copy All' and 'Close', and a checkbox for 'Next Highlighted'.

Module	Address	Size	Path	Company	Version	Ti
svchost.exe	0x7ff62eee0000	0x11000	C:\WINDOWS\system32\svchost.exe	Microsoft Cor...	10.0.22621.1 (...	5...
windows.statel...	0x7fff1cde0000	0x3d000	C:\WINDOWS\SYSTEM32\window...	Microsoft Cor...	10.0.22621.457 ...	11...
Windows.State...	0x7fff25750000	0xeb000	C:\Windows\System32\Windows....	Microsoft Cor...	10.0.22621.457 ...	6...
windows.statel...	0x7fff27190000	0x1a000	C:\WINDOWS\SYSTEM32\window...	Microsoft Cor...	10.0.22621.457 ...	4...
StateRepository...	0x7fff27250000	0xb3000	c:\windows\system32\StateRepos...	Microsoft Cor...	10.0.22621.457 ...	11...
windows.statel...	0x7fff27380000	0x682000	c:\windows\system32\windows.st...	Microsoft Cor...	10.0.22621.1 (...	1...

Running Malware-Process Monitor

 To narrow the result, use filtering

 You may want to filter on:

Executables running on the system

System call (such as RegSetValue, Create File, WriteFile, etc.)

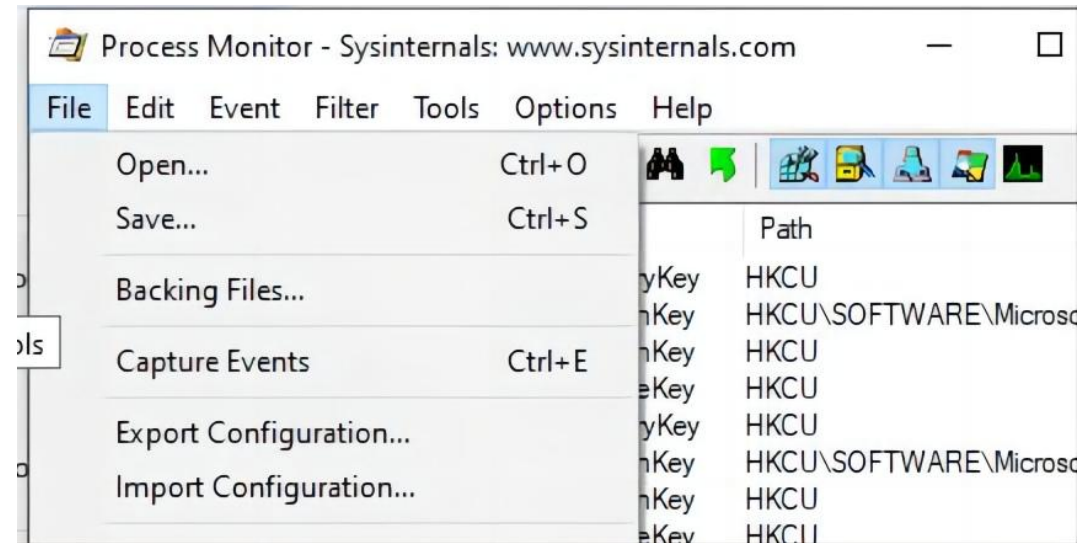
Note: Filtering does not prevent from consuming too much memory though.



Example1-Track File and Registry Changes

- Let's say, you need to track access to the registry key `HKEY_CURRENT_USER\Software\test` and file `c:\ps\procmon_example.txt`.
- When Process Monitor starts, it begins capturing all events according to the default filters.

- Step 1. Stop capturing events by unchecking the option File > Capture Events (Ctrl+E).
- Step 2. Clear the current ProcMon log (Edit > Clear Display).



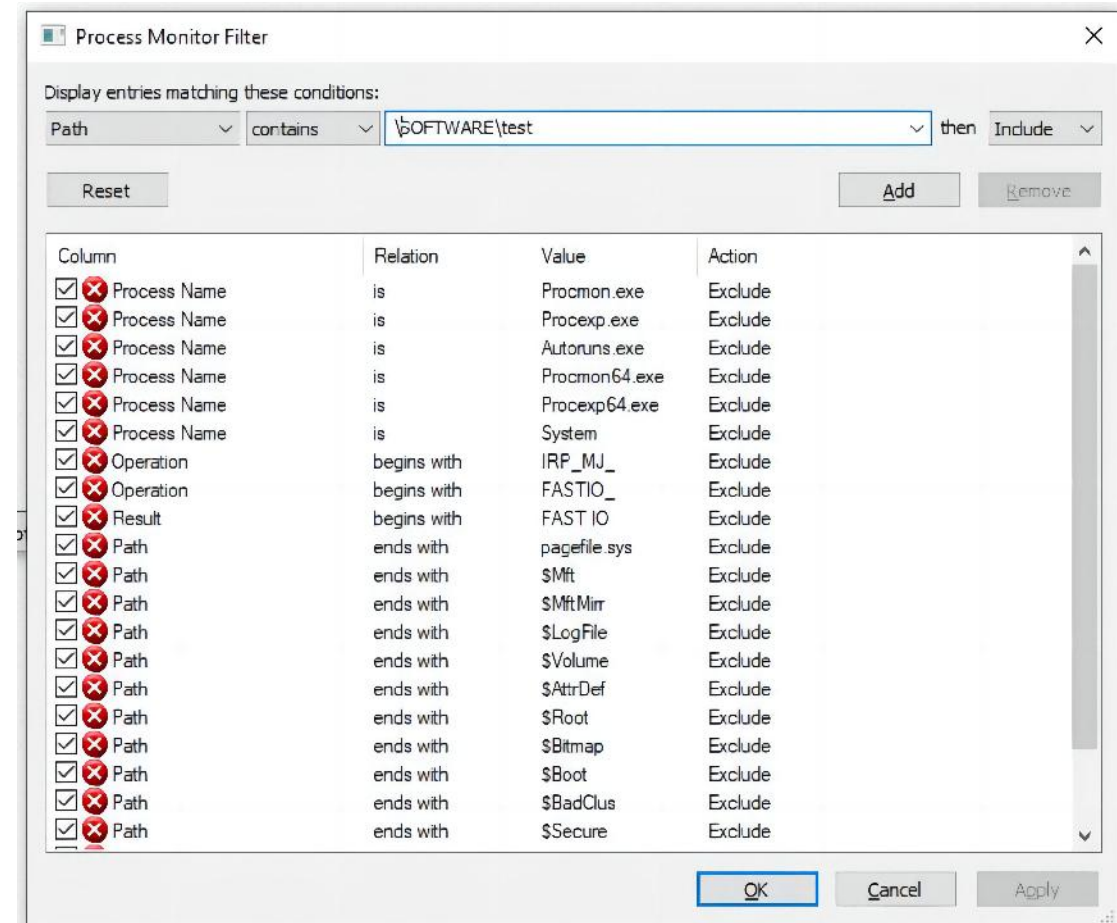


Example1-Track File and Registry Changes



Let's say, you need to track access to the registry key HKEY_CURRENT_USER\Software\test and file c:\ps\procmon_example.txt.

- ❑ Step 3. Now you need to configure the Process Monitor filters (Filter > Filter).
- ❑ Step 4. Create a filter for monitoring access to the registry key: Path > contains > \SOFTWARE\test > Include.
- ❑ Step 5. Click Add to add a new filter to the list



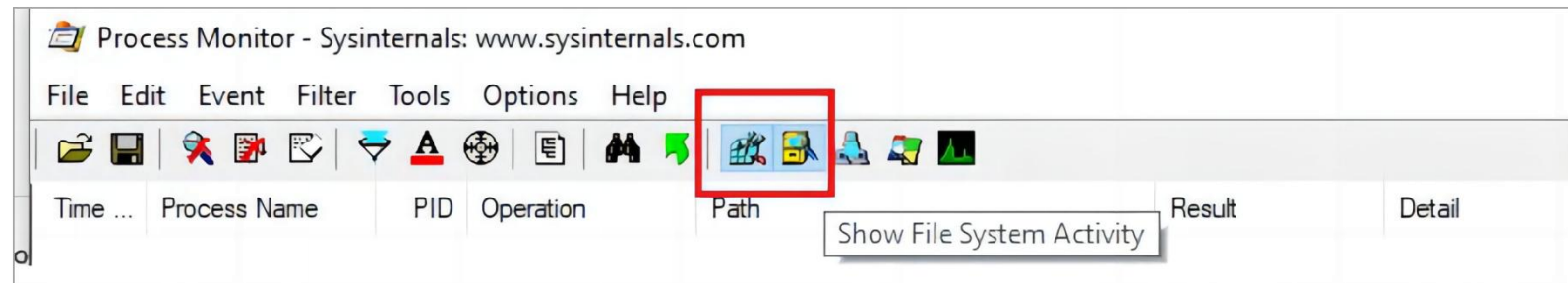


Example1-Track File and Registry Changes



Let's say, you need to track access to the registry key HKEY_CURRENT_USER\Software\test and file c:\ps\procmon_example.txt.

- ❑ Step 6. Now add a file access event filter: Path > is > c:\ps\procmon_example.txt > Include.
- ❑ Step 7. Make sure the following options are enabled in the toolbar: Show Registry Activity, Show File System Activity.
- The Show Network Activity and Show Process, and Threads Activity options can be disabled.





Example1-Track File and Registry Changes



Let's say, you need to track access to the registry key `HKEY_CURRENT_USER\Software\test` and file `c:\ps\procmon_example.txt`.

- ❑ Step 8. Start event monitoring File > Capture Event.
- ❑ Step 9. Let's create a reg parameter key in the specified registry key using the **command prompt**:
 - `reg add hkcu\software\test /v Path /t REG_EXPAND_SZ /d ^%systemroot^%`
- ❑ Step 10. Let's write some data into the `procmon_example.txt` file using the **command prompt**:
 - `echo %date%>>c:\ps\procmon_example.txt`
- ❑ Step 11. And using **PowerShell**:
 - `Get-Process|out-file C:\ps\procmon_example.txt`



Example1-Track File and Registry Changes



Let's say, you need to track access to the registry key HKEY_CURRENT_USER\Software\test and file c:\ps\procmon_example.txt.

- ❑ It contains events for creating a registry key by the reg.exe process (Operation > RegCreateKey).
- ❑ It also contains events of creation (Create File) and writing to a file (WriteFile) by the processes cmd.exe and powershell.exe.

Time ...	Process Name	PID	Operation	Path	Result	Detail
17:50:...	reg.exe	11612	RegCreateKey	HKCU\software\test	SUCCESS	Desired Access: R...
17:50:...	reg.exe	11612	RegQueryValue	HKCU\SOFTWARE\test\Path	NAME NOT FOUND	Length: 12
17:50:...	reg.exe	11612	RegSetValue	HKCU\SOFTWARE\test\Path	SUCCESS	Type: REG_EXPA...
17:50:...	reg.exe	11612	RegCloseKey	HKCU\SOFTWARE\test	SUCCESS	
17:52:...	cmd.exe	10208	CreateFile	C:\PS\procmon_example.txt	NAME NOT FOUND	Desired Access: G...
17:52:...	cmd.exe	10208	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: G...
17:52:...	cmd.exe	10208	QueryStandardInformationFile	C:\PS\procmon_example.txt	SUCCESS	AllocationSize: 0. E...
17:52:...	cmd.exe	10208	WriteFile	C:\PS\procmon_example.txt	SUCCESS	Offset: 0, Length: 1...
17:52:...	cmd.exe	10208	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:52:...	MsMpEng.exe	5352	CreateFileMapping	C:\PS\procmon_example.txt	FILE LOCKED WI...	SyncType: SyncTy...
17:52:...	MsMpEng.exe	5352	QueryStandardInformationFile	C:\PS\procmon_example.txt	SUCCESS	AllocationSize: 16, ...
17:52:...	MsMpEng.exe	5352	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: R...
17:52:...	MsMpEng.exe	5352	QueryNetworkOpenInformationFile	C:\PS\procmon_example.txt	SUCCESS	CreationTime: 23/1...
17:52:...	MsMpEng.exe	5352	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:52:...	MsMpEng.exe	5352	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: R...
17:52:...	MsMpEng.exe	5352	FileSystemControl	C:\PS\procmon_example.txt	OPLOCK HANDLE...	Control: FSCTL_R...
17:52:...	MsMpEng.exe	5352	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: G...
17:52:...	MsMpEng.exe	5352	QueryStandardInformationFile	C:\PS\procmon_example.txt	SUCCESS	AllocationSize: 16, ...
17:52:...	MsMpEng.exe	5352	QueryBasicInformationFile	C:\PS\procmon_example.txt	SUCCESS	CreationTime: 23/1...
17:52:...	MsMpEng.exe	5352	FileSystemControl	C:\PS\procmon_example.txt	SUCCESS	Control: FSCTL_R...
17:52:...	MsMpEng.exe	5352	QueryBasicInformationFile	C:\PS\procmon_example.txt	SUCCESS	CreationTime: 23/1...
17:52:...	MsMpEng.exe	5352	ReadFile	C:\PS\procmon_example.txt	SUCCESS	Offset: 0, Length: 1...
17:52:...	MsMpEng.exe	5352	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:52:...	MsMpEng.exe	5352	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:52:...	powershell.exe	9092	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: R...
17:52:...	powershell.exe	9092	QueryNetworkOpenInformationFile	C:\PS\procmon_example.txt	SUCCESS	CreationTime: 23/1...
17:52:...	powershell.exe	9092	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:53:...	powershell.exe	9092	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: R...
17:53:...	powershell.exe	9092	QueryBasicInformationFile	C:\PS\procmon_example.txt	SUCCESS	CreationTime: 23/1...
17:53:...	powershell.exe	9092	CloseFile	C:\PS\procmon_example.txt	SUCCESS	
17:53:...	powershell.exe	9092	CreateFile	C:\PS\procmon_example.txt	SUCCESS	Desired Access: G...
17:53:...	powershell.exe	9092	WriteFile	C:\PS\procmon_example.txt	SUCCESS	Offset: 0, Length: 7...
17:53:...	powershell.exe	9092	WriteFile	C:\PS\procmon_example.txt	SUCCESS	Offset: 732, Length...
17:53:...	powershell.exe	9092	WriteFile	C:\PS\procmon_example.txt	SUCCESS	Offset: 974, Length...

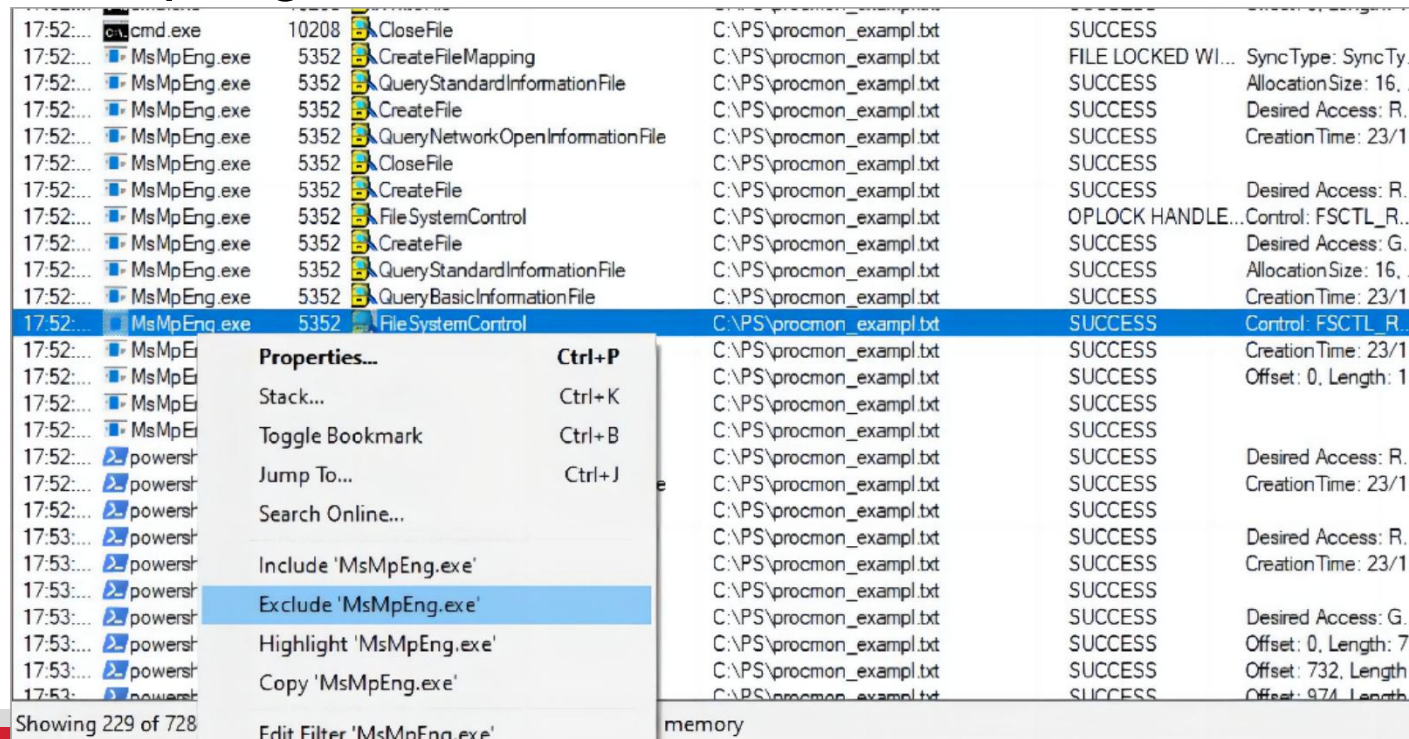
Showing 229 of 579,404 events (0.039%)

Backed by virtual memory


Example2-Exclude System Process

 Let's say, exclude **msmpeng.exe** (Antimalware Service Executable). This is the core process of the antimalware detection engine in Windows Defender.

- ❑ To exclude the events of this process from the ProcMon log, right-click on the process name msmpeng.exe and select Exclude.



Example2-Exclude System Process

 Let's say, exclude **msmpeng.exe** (Antimalware Service Executable). This is the core process of the antimalware detection engine in Windows Defender.

☐ This process will be added to the ProcMon filter with the Exclude value. It means that the ProcMon log won't display any activity from this process.

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process Name	is	Procexp64.exe	Exclude
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process Name	is	System	Exclude
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process Name	is	MsMpEng.exe	Exclude
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	begins with	IRP_MJ_	Exclude
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	begins with	FASTIO_	Exclude
<input type="checkbox"/>	<input checked="" type="checkbox"/>				



Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-931HL8C\defaultuser0]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		3,160 K	11,344 K	2528	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,312 K	5,092 K	2536	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,080 K	5,876 K	2552	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,036 K	5,796 K	2524	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,348 K	7,805 K	2568	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,776 K	10,655 K	2576	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,040 K	14,283 K	2956	Host Process for Windows S...	Microsoft Corporation
audodg.exe		7,740 K	14,216 K	10544		
svchost.exe		1,552 K	5,980 K	2364	Host Process for Windows S...	Microsoft Corporation
cfmmon.exe		23,156 K	31,996 K	7364		
svchost.exe		2,884 K	7,664 K	3052	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,208 K	9,560 K	3060	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,720 K	6,292 K	3068	Host Process for Windows S...	Microsoft Corporation
svchost.exe		26,860 K	18,160 K	2152	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,572 K	11,036 K	2976	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,452 K	7,520 K	3164	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,884 K	9,400 K	3252	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		8,048 K	15,884 K	3308	Spooler Sub-System App	Microsoft Corporation
svchost.exe		11,356 K	15,695 K	3332	Host Process for Windows S...	Microsoft Corporation
svchost.exe		43,480 K	40,944 K	3440	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,136 K	8,756 K	3448	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,276 K	4,628 K	3456	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,152 K	11,740 K	3464	Host Process for Windows S...	Microsoft Corporation
shost.exe		7,012 K	31,795 K	5420	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		8,940 K	18,564 K	3472	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,440 K	7,972 K	3864	Host Process for Windows S...	Microsoft Corporation
AsusUpdateCheck.exe		3,032 K	10,480 K	4060	WPBT_with_NoDriver	
MsMpEng.exe	< 0.01	395,856 K	223,580 K	5060	Antimalware Service Execut...	Microsoft Corporation
SearchIndexer.exe		45,296 K	35,860 K	4512	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.c...		1,736 K	8,492 K	21364	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe		1,796 K	5,844 K	15016		
SearchFilterHost.exe		2,044 K	7,804 K	30340		
SearchProtocolHost.e...		2,808 K	12,612 K	26180		
svchost.exe		6,160 K	14,060 K	2144	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		45,772 K	65,176 K	5720		
svchost.exe		3,736 K	13,496 K	2544	Host Process for Windows S...	Microsoft Corporation
NisSrv.exe		9,076 K	12,143 K	4312	Microsoft Network Realtime I...	Microsoft Corporation
svchost.exe		1,996 K	5,983 K	4592	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,760 K	9,204 K	4568	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,400 K	19,176 K	4580	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,068 K	19,700 K	4900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,692 K	11,723 K	5272	Host Process for Windows S...	Microsoft Corporation
svchost.exe		21,956 K	28,880 K	5580	Host Process for Windows S...	Microsoft Corporation
AggregatorHost.exe		3,024 K	8,676 K	5548		
svchost.exe		2,654 K	8,043 K	6136	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,788 K	12,244 K	5292	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,816 K	14,423 K	3528	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,112 K	19,084 K	5348	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,528 K	6,156 K	3428	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,960 K	13,472 K	6156	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,048 K	33,116 K	6196	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,668 K	11,595 K	5356	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,540 K	18,200 K	6580	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,888 K	21,943 K	6580	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,668 K	12,504 K	4320	Host Process for Windows S...	Microsoft Corporation
SecurityHealthService.exe		3,904 K	16,020 K	6516	Windows Security Health Se...	Microsoft Corporation

svchost.exe:2956 (LocalServiceNetworkRestricted -p) Pro...

Image Performance Performance Graph GPU Graph Services
Threads TCP/IP Security Environment Strings

Printable strings found in the scan:

uRH
D\$PH;
D9-nT
QRA
D\$PH,
D\$PH
AHL3ABs
qSR
qSR
wAL
ServiceMain
SvcHostPushServiceGlobaleEx
SvcHostPushServiceGlobale
WdplAllowedEntryPoint
api-ms-win-service-private-l1-1-3.dll
api-ms-win-service-winsock-l1-1-0.dll
api-ms-win-service-core-l1-1-0.dll
api-ms-win-core-comm-l1-1-0.dll
RPCRT4.dll
NoUrlMimeFilters
ETW0
Calling_ExitProcess
CommandLine
SleepConditionVariableSRW_Failed
ServiceName
ErrorCode
UnloadingServiceDll

Image Memory Save End OK Cancel

wininit.exe:1040 Properties

TCP/IP Security Environment Strings
Image Performance Performance Graph GPU Graph Threads

Count: 2

TID	CPU	CSwitch D...	Suspend Count	Start Address
1044				!RtlUserThreadStart
1228				!RtlUserThreadStart

Thread ID:
Start Time:
State:
Kernel Time:
User Time:
Context Switches:
Cycles:

Base Priority:
Dynamic Priority:
I/O Priority:
Memory Priority:
Ideal Processor:

Permissions Kill Suspend OK Cancel

Process Explorer Vs. Process Monitor

Process Explorer

- Shows current state of each process
- Shows files, registry keys and thread loaded by each running process

Process Monitor

- In addition to monitoring, it logs process information- all events
- Logs show the file, registry, network, etc. the process attempted to use
 - successful or not
- “Access Denied” events also appear



Monitoring Network Activities

WHY?



➤➤ Most malware will need to communicate with external services/entities.

Download additional malware, files

Exchange/obtain keys for encryption

C2-Command and Control: Receive instructions and check-in

Extract data

Infect other machines

➤➤ **Question:** Do we allow them access to network?



Faking a Network

- 💎 It is too risky to allow a malware to access the network.
- 💎 Faking a network allows us to find out how/what is communicated.
- 💎 **Important:** Faking requires that the malware does not realize it is executing on a virtualized environment.





Faking a Network-FakeNet



An open source tool.



Allow users to intercept and redirect all or specific network traffic.



You can identify malware functionality and capture network signatures.





Faking a Network-FakeNet

- 1. Fakenet takes over DNS on port 53.
- 2. It listens to the TCP ports 80, 443 and 25.
- 3. It supports DNS, HTTP and SSL protocols.





FakeNet-Use



1. Stop most programs that connect to the Internet prior to running Fakenet.



2. Just run the program you want to analyze.



3. Still get some noise from Windows itself and maybe background processes that you cannot just terminate.

```
Select C:\Users\defaultuser0\DESKTOP-931HL80\Downloads\Fakenet1.0c\Fakenet1.0b\FakeNet.exe

[Received new connection on port: 80.]
[New request on port 80.]
GET /wpad.dat HTTP/1.1
Host: wpad
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.20 Safari/537.36
Accept-Encoding: gzip, deflate

[Received new connection on port: 80.]
Accept-Language: en-US,en;q=0.9

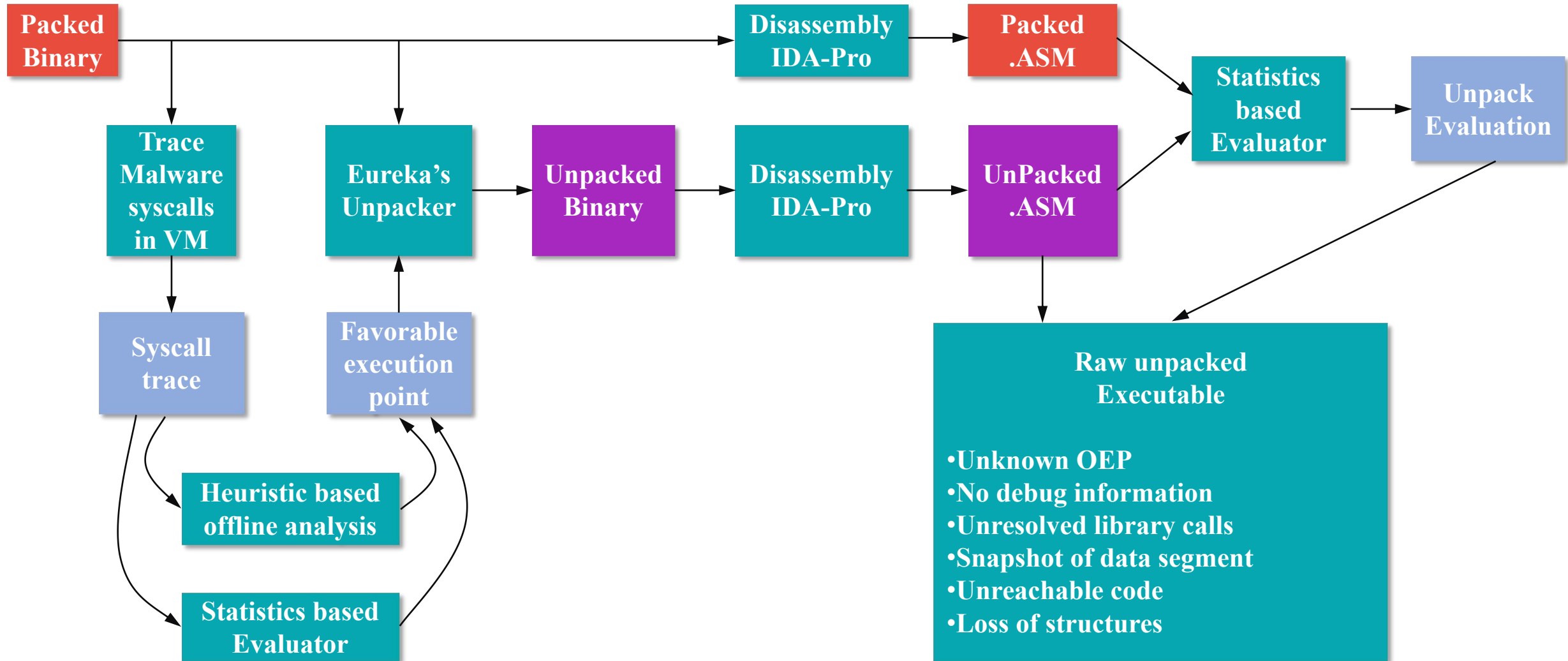
[New request on port 80.]
GET /wpad.dat HTTP/1.1
Host: wpad
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.20 Safari/537.36
Accept-Encoding: gzip, deflate

[Failed to open file C:\Users\defaultuser0\DESKTOP-931HL80\Downloads\Fakenet1.0c\Fakenet1.0b\defaultFiles\FakeNet.html to respond to HTTP request.]
[Sent http response to client.]

[DNS Query Received.]
Domain name: mozilla.cloudflare-dns.com
[DNS Response sent.]
```

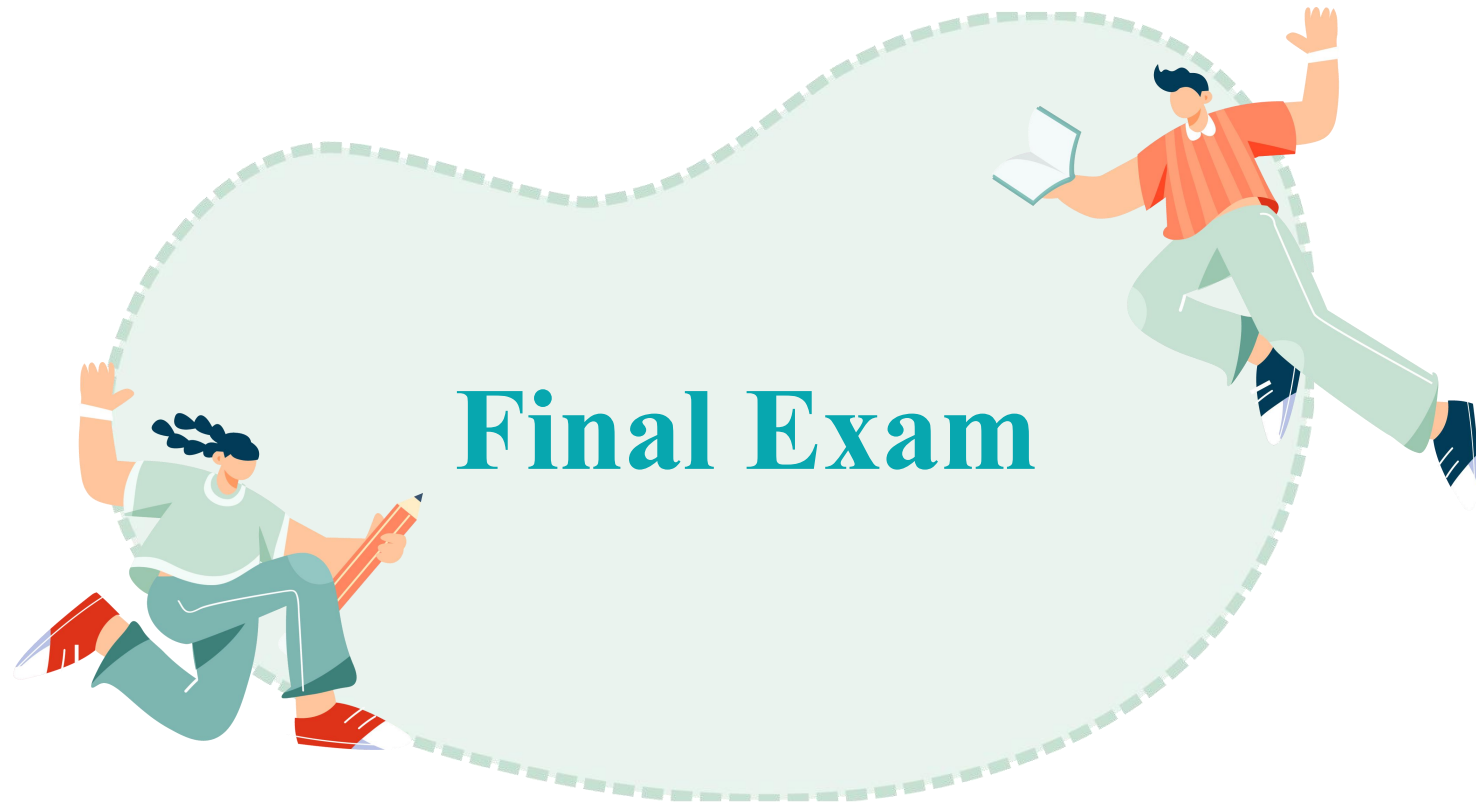



The Eureka Workflow





Questions



THE END

Fangtian Zhong

CSCI 591

Gianforte School of Computing
Norm Asbjornson College of Engineering
E-mail: fangtian.zhong@montana.edu

11/20/2025