BFOR - 418/618 - Reverse Engineering Malware
Basic Dynamic Analysis

Katta Sreenivasulu, Tarun Sai

October 12, 2023

Dr. Prinkle Sharma
University at Albany, SUNY

Contents

1 Introduction

In this lab, Basic Dynamic analysis is performed using tools mentioned below

1. **Regshot** - To compare the changes in files and keys.
2. **Procmon** - To see real-time file system, Registry and process/thread activity.
3. **WireShark** - To perform network packet sniffing.
4. **FakeNet-ng** - To intercept and redirect all or specific network traffic while simulating legitimate network services.

2 Basic Dynamic Analysis

Dynamic analysis involves examining and analyzing malware after executing or running it. It mainly focuses on understanding the true functionality of malware, which cannot be determined using static analysis techniques to packed or obfuscation.

Dynamic analysis is extremely powerful and to be performed only after static analysis. There is always the risk of malware infecting both network and system after execution if sample is not contained.

Pro's:

1. **Behavioral Analysis:** Dynamic analysis allows for observing the behavior of malware in a controlled environment, providing insights into its actions, communication, and potential damage it could cause. This helps in understanding the threat's capabilities and intentions.
2. **Detection of Evasive Techniques:** Dynamic analysis can help in detecting malware's attempts to evade detection or analysis, such as employing anti-analysis or anti-debugging techniques. Identifying these evasion tactics can aid in developing countermeasures.
3. **Rapid Analysis:** Dynamic analysis is generally quicker compared to static analysis (where code is analyzed without executing it). It provides a faster way to identify malware behavior and patterns, which is crucial for timely response and mitigation.

4. **Sample Variability:** Dynamic analysis allows for analyzing a wide range of malware samples, providing insights into the variability and sophistication of attacks. This helps in improving threat intelligence and adapting defenses to evolving attack vectors.

Con's:

1. **Limited Visibility:** Dynamic analysis might not fully reveal the entire scope of the malware's capabilities, as some malicious actions may be triggered conditionally with command-line arguments or might require specific environmental conditions like Sleep for a day and then perform another action, that are not replicated during analysis.

2. **Resource Intensive**: Running malware in a controlled environment can be resource-intensive, requiring specialized hardware and software setups. This can be costly and time-consuming, especially for large-scale or continuous analysis.

3. **False Negatives:** Malware might exhibit different behaviors in a controlled environment compared to a real-world scenario, leading to potential false negatives. It might miss certain behaviors that only manifest in specific conditions.

4. **Evasion and Obfuscation:** Sophisticated malware can detect when it's being analyzed and modify its behavior to appear benign, making it difficult to capture its true malicious intent. Additionally, malware may use various obfuscation techniques to hide its true nature during dynamic analysis.

3 Software Used

(i) **RegShot** is an open source registry comparison tool that allows to take and compare two registry snapshots.

(ii) **Procmon** is an advanced monitoring tool for Windows that provides a way to monitor certain registry, file system, network, process, and thread activity in real-time.

(iii) **WireShark** is an open source packet sniffer or a packet capture tool that intercepts and logs network traffic.

(iv) **FakeNet-ng** allows to intercept and redirect all or specific network traffic while simulating legitimate network services.

(v) **PE Explorer** is a tool that allows to view, examine and edit EXE and DLL files, or any executable files.

(vi) **AutoRuns** is a utility with a long list of auto starting locations for Windows

4 Methodology

To analyse the malware samples and perform basic dynamic analysis, it is required to posses the tools mentioned in previous section ready and installed in virtualized windows environment.

Firstly, disconnect from internet and with the network adapter provided to virtual machine environment using **FakeNet-ng**, all the network traffic is intercepted and redirected.

4.1 Analyzing Malware file re_whatami.exe

4.1.1 RegShot:

To use regshot, simply take 1st shot, run the malware and take 2nd shot and hit compare to check changes made by malware sample. Here, to check the changes made to files and directories, the root directory of windows operating system **C:** is scanned.

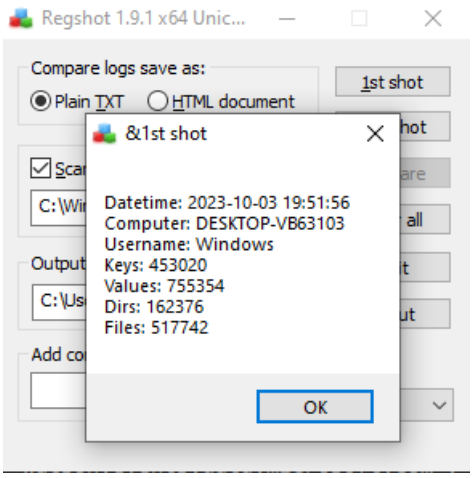

Figure 1: 1st Shot in Regshot before executing re_whatami.exe

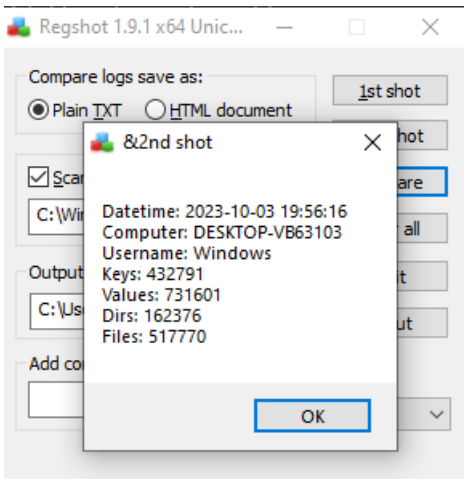

Figure 2: 2nd Shot in Regshot after executing re_whatami.exe

After comparing the 2nd shot which is taken after executing the malware sample re_whatami.exe, with 1st shot, it is clear that the malware has deleted few keys and added files in the host system.

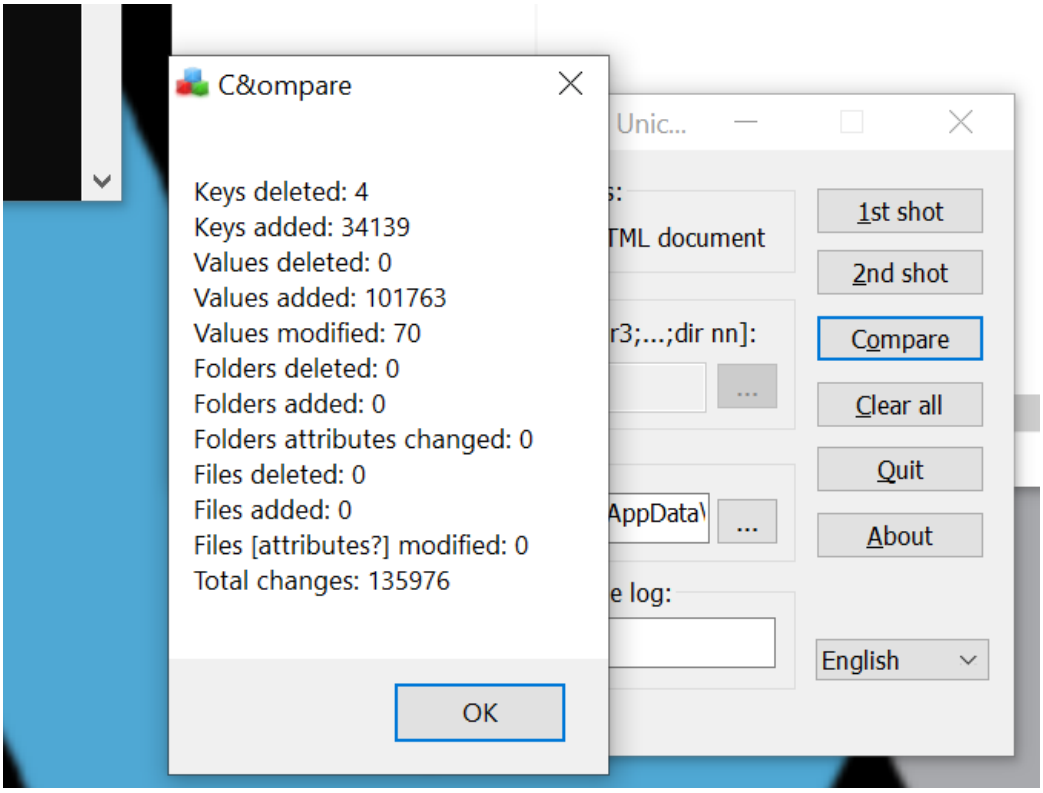

Figure 3: Compare shot for re_whatami.exe

4.1.2 Procmon

After careful analysis of the process tree, registry keys, using the Process Tree Filter options, it will be easy to filter the processes created from re_whatami.exe.

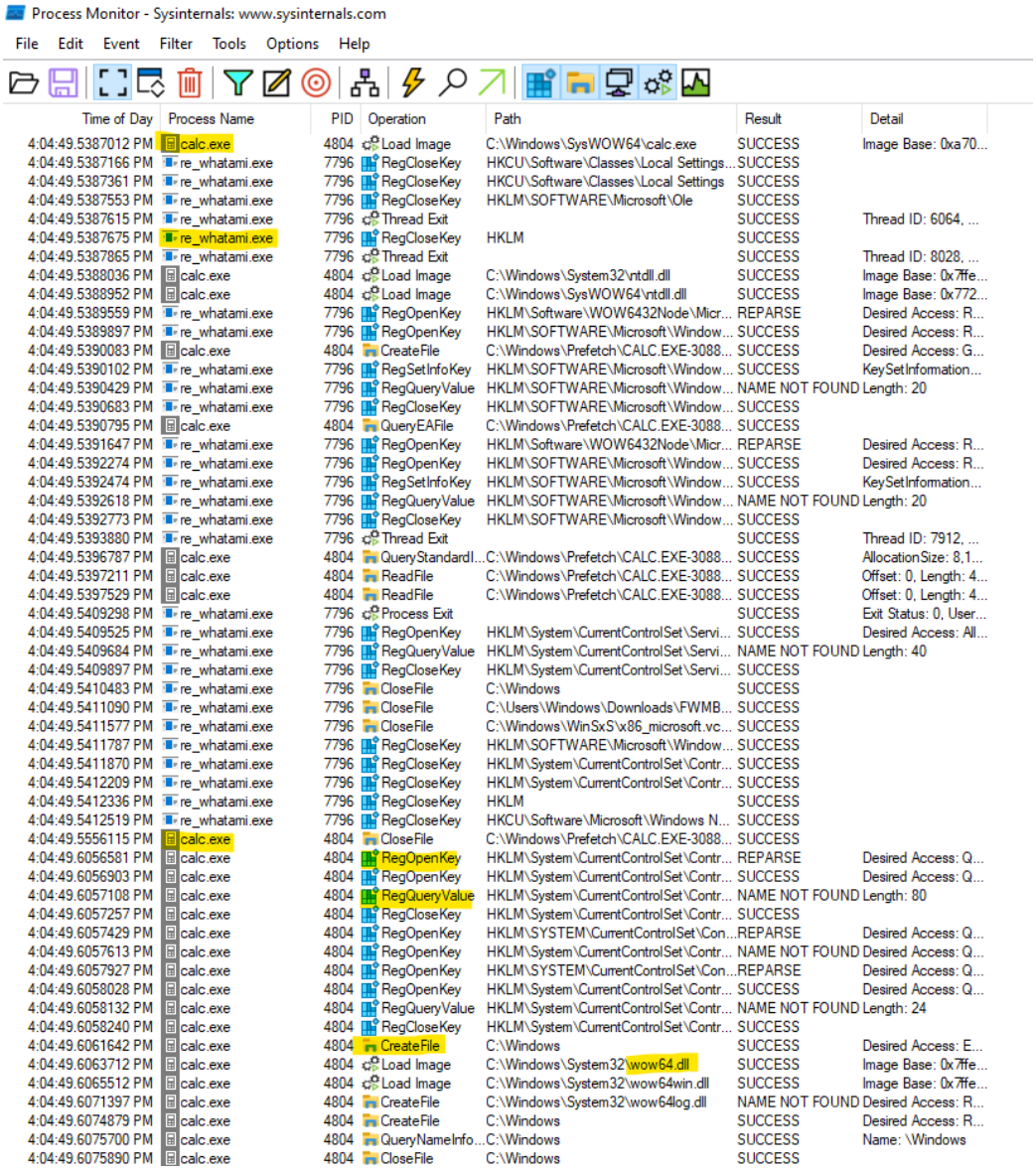

Figure 4: Procmon for re_whatami.exe

From Figure 4, **re_whatami.exe** is running with PID of 7796, which also started a new process **calc.exe** with PID 4804, where it is performing operations like **RegOpenKey** and **RegQueryValue**.

4.1.3 FakeNet-NG

FakeNet-ng is used to intercept and redirect all or specific network traffic while simulating legitimate network services.

Before executing malware, it is advised to make sure connection to internet is disabled with network adapter still up and running FakeNet-ng on that network adapter.

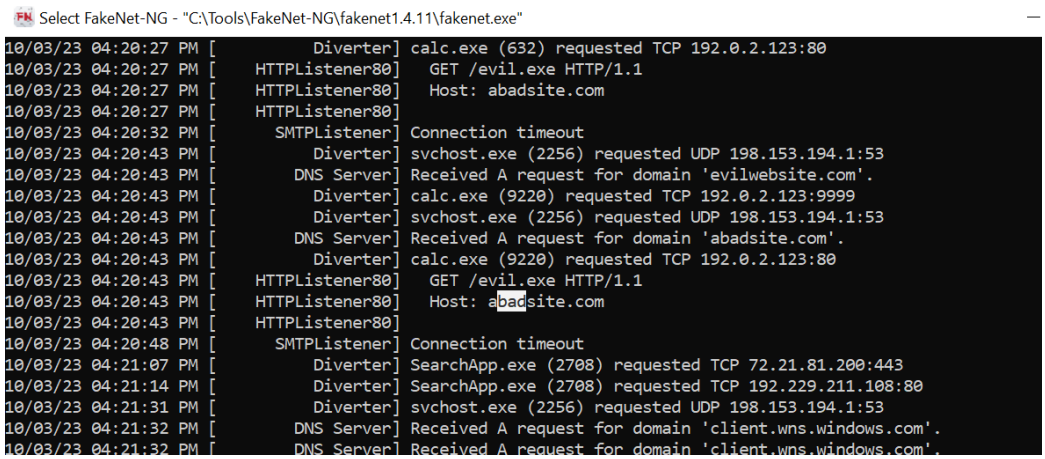

Figure 5: FakeNet-NG Intercepting traffic to badsite

4.1.4 Wireshark

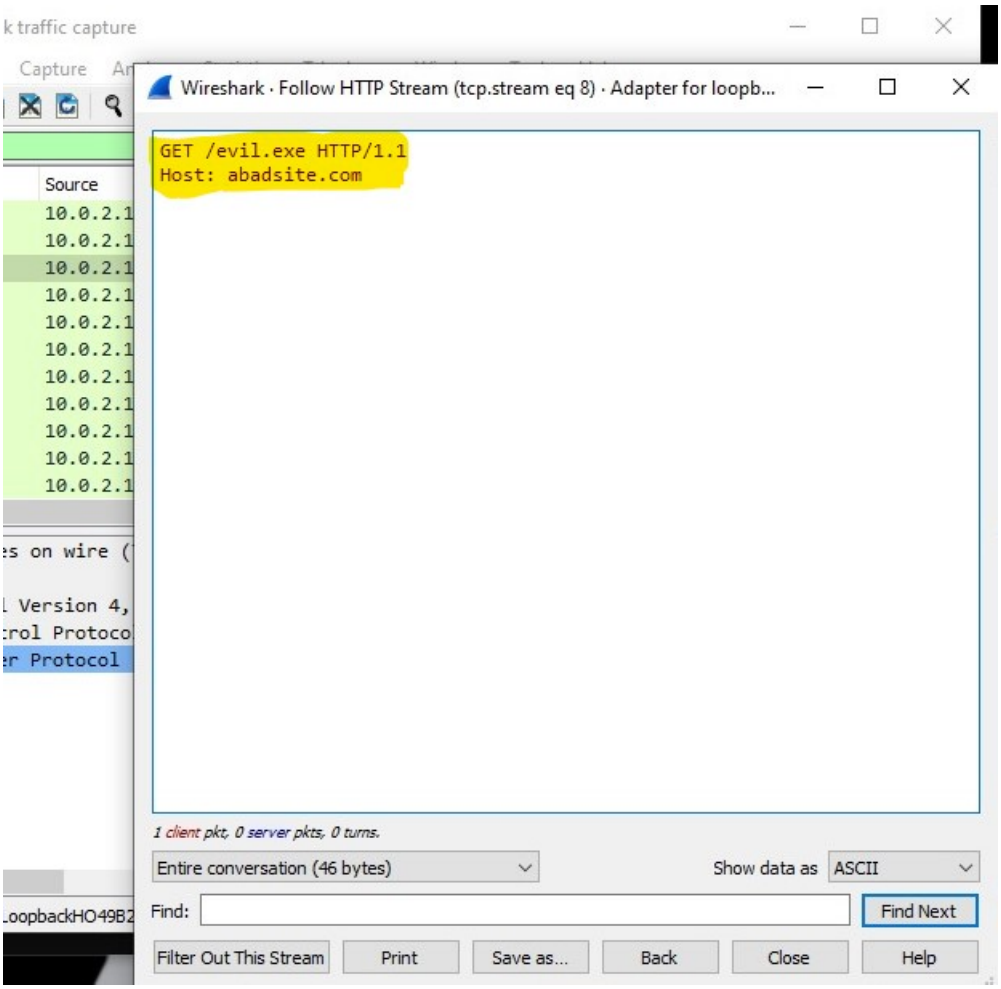

Figure 6: After following HTTP Stream in Wireshark tool

4.2 Analyzing file Lab03-03.exe

1. **What do you notice when monitoring this malware with Process Explorer?**

   The malware is trying to create a subprocess **svchost.exe** and exits, making it an orphan.

2. **Can you identify any live memory modifications?**

   In **Process Explorer**, right-click on **svchost.exe**, selecting **Properties**, reveals the tab where one can check for Strings. By comparing with image and memory, it is understood that it is not the same, memory image has Strings like **practicemalwareanalysis.log**, but disk image does not have it.

3. **What are the malware's host-based indicators?**

   It creates a log file named **practicemalwareanalysis.log**

4. **What is the purpose of this program?**

   The executable appears to be exploiting an orphaned process and creating a log file.

4.3 Analyzing re_test_dlx.doc using AutoRuns Utility

First, to support the doc file, Word processor software like Microsoft word or LibreOffice must be installed in environment.

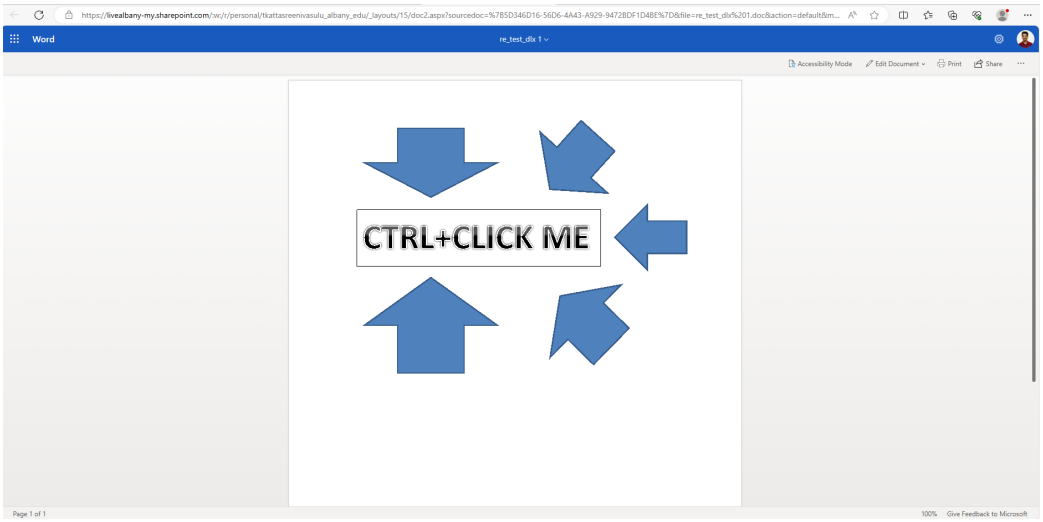

Figure 7: Word Document contents

Click on the box, which will redirect to a site as shown in Figure 8 below.

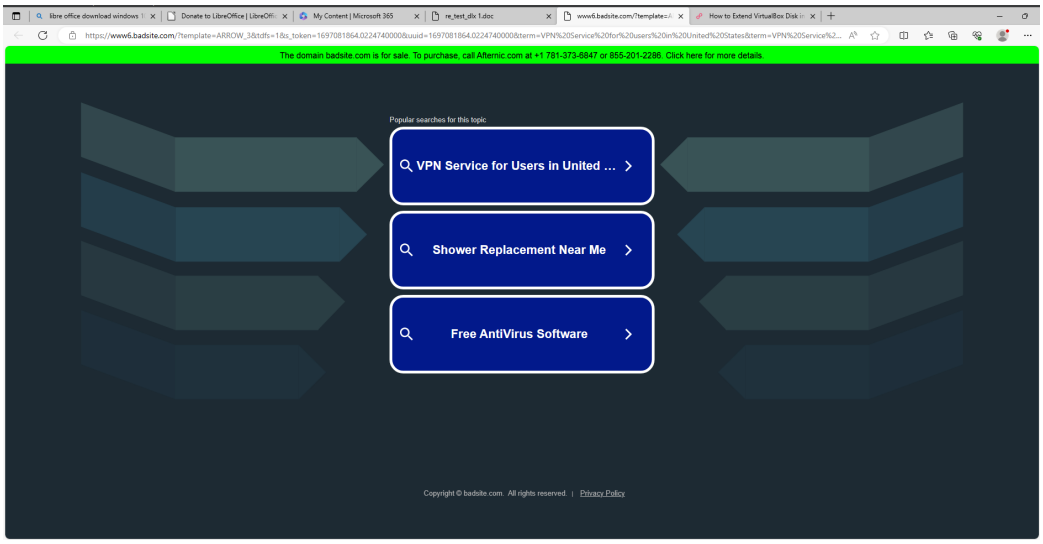

Figure 8: Badsite link from Word Document

While executing the **.doc** file, open AutoRuns utility in background to check for autostarting programs from multiple processes.

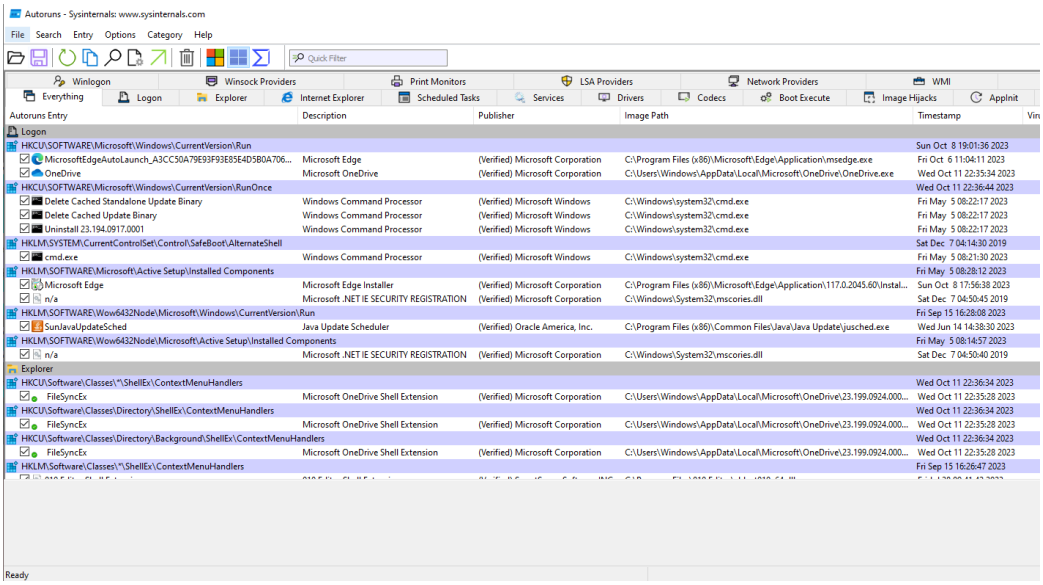

Figure 9: AutoRuns Utility output for re_test_dlx.doc

From the Figure 9, it is understood that the malware is creating a temporary Registry Persistance using **HKCU\SOFTWARE \Microsoft \Windows \CurrentVersion \Run** Registry Key.

5 Conclusion

Dynamic Analysis provides a real-time glimpse into the behavior and intentions of malicious software in a controlled environment. By executing malware and observing its actions, One can uncover vital insights, such as communication protocols, evasion tactics, and potential damage it could inflict.

Using tools like FakeNet-ng, it helps in intercepting the network traffic and thereby reducing the interaction with an actual internet and other devices in the network.

With RegShot, comparing the shots before executing the malware and after executing the malware, it provides insights on the number of changes done on the system, be it files, directories, registry keys and values.

Using Wireshark, the entire network traffic can be intercepted and filtered based on the parameters like **Follow TCP Stream** to filter out the TCP stream data to see how the packets are being transferred after establishing a TCP Connection with a random Website or server.

However, basic dynamic analysis techniques have their deficiencies, so analysts proceed with advanced dynamic analysis using techniques like debugging and analysing the executable file with disassemblers like IDA Pro.