Digital Forensics Investigation Report

Title: Comprehensive Forensic Analysis and Timeline Reconstruction of a Windows 10 Virtual Machine
Student Name: Loksharan Saravanan
Course: Digital Forensics
Instructor: [Insert Instructor Name]
Date: [Insert Date]

Table of Contents

1. Abstract
2. Introduction
3. Background and Theoretical Foundations
4. Scope of Investigation
5. Tools and Environment
   5.1 Target System
   5.2 Analysis System
   5.3 Forensic Tools
6. Incident Simulation
   6.1 File Creation, Modification, and Deletion
   6.2 Suspicious Program Execution
   6.3 PowerShell Simulation
   6.4 Web Activity and Downloads
   6.5 Data Staging and Exfiltration Simulation
   6.6 Registry Manipulation Simulation
   6.7 Event Log Simulation
   6.8 Summary
7. Evidence Acquisition
   7.1 Disk Imaging Procedure
   7.2 Hashing and Integrity Verification
8. Chain of Custody
9. Forensic Analysis
   9.1 Autopsy Case Setup
   9.2 Filesystem and Deleted Files Analysis
   9.3 Windows Registry Analysis
   9.4 Browser Artifact Analysis
   9.5 Log Analysis
10. Timeline Reconstruction
11. Findings
12. Challenges and Limitations
13. Learning Outcomes
14. Conclusion
15. References

16. Appendices
    16.1 Appendix A: Full Command List
    16.2 Appendix B: Hash Values
    16.3 Appendix C: Timeline CSV Output
    16.4 Appendix D: Additional Screenshots

---

6. Incident Simulation

6.1 File Creation, Modification, and Deletion

PowerShell Commands:

```
# Create a test file
New-Item -Path C:\Users\vboxuser1\Documents\incident_test.txt -ItemType File

# Copy the file to Desktop
Copy-Item -Path C:\Users\vboxuser1\Documents\incident_test.txt -Destination C:
\Users\vboxuser1\Desktop\incident_copy.txt

# Display contents of copied file
Get-Content -Path C:\Users\vboxuser1\Desktop\incident_copy.txt

# Delete original file
Remove-Item -Path C:\Users\vboxuser1\Documents\incident_test.txt
```

Screenshot Placeholder: PowerShell showing commands and outputs

6.2 Suspicious Program Execution

```
# Navigate to Downloads
Set-Location C:\Users\vboxuser1\Downloads

# Launch Notepad (test program)
Start-Process notepad.exe
```

Screenshot Placeholder: PowerShell showing program execution

6.3 PowerShell Simulation

```
# Create file using PowerShell
New-Item -Path C:\Users\vboxuser1\Documents\ps_test.txt -ItemType File
```

```
# List all files and export output
Get-ChildItem -Path C:\Users\vboxuser1\Documents | Out-File -FilePath C:
\Users\vboxuser1\Documents\ps_output.txt
```

Screenshot Placeholder: PowerShell commands and output

6.4 Web Activity and Downloads

```
# List files in Downloads folder
Get-ChildItem -Path C:\Users\vboxuser1\Downloads
```

Screenshot Placeholder: Downloaded files and timestamps

6.5 Data Staging

```
# Export directory listing of Documents folder to Desktop
Get-ChildItem -Path C:\Users\vboxuser1\Documents | Out-File -FilePath C:
\Users\vboxuser1\Desktop\staged_data.txt
```

Screenshot Placeholder: PowerShell output of staged data

6.6 Registry Manipulation

```
# Add a simulated registry key
New-Item -Path HKCU:\Software\IncidentSimulation
New-ItemProperty -Path HKCU:\Software\IncidentSimulation -Name TestValue -Value
SimulatedEntry -PropertyType String

# Remove registry key
Remove-ItemProperty -Path HKCU:\Software\IncidentSimulation -Name TestValue
Remove-Item -Path HKCU:\Software\IncidentSimulation
```

Screenshot Placeholder: PowerShell and regedit showing registry changes

6.7 Event Log Simulation

```
# Create application and system events
New-EventLog -LogName Application -Source IncidentSim
Write-EventLog -LogName Application -Source IncidentSim -EventID 100 -EntryType
Information -Message "Simulated application event"
```

```
New-EventLog -LogName System -Source IncidentSim
Write-EventLog -LogName System -Source IncidentSim -EventID 101 -EntryType
Information -Message "Simulated system event"
```

Screenshot Placeholder: Event Viewer entries filtered by IncidentSim

6.8 Summary

All simulated actions produced artifacts across filesystem, registry, browser data, PowerShell logs, and Windows event logs, forming a comprehensive dataset for forensic analysis. **Screenshot Placeholder:** Overview of all simulation artifacts