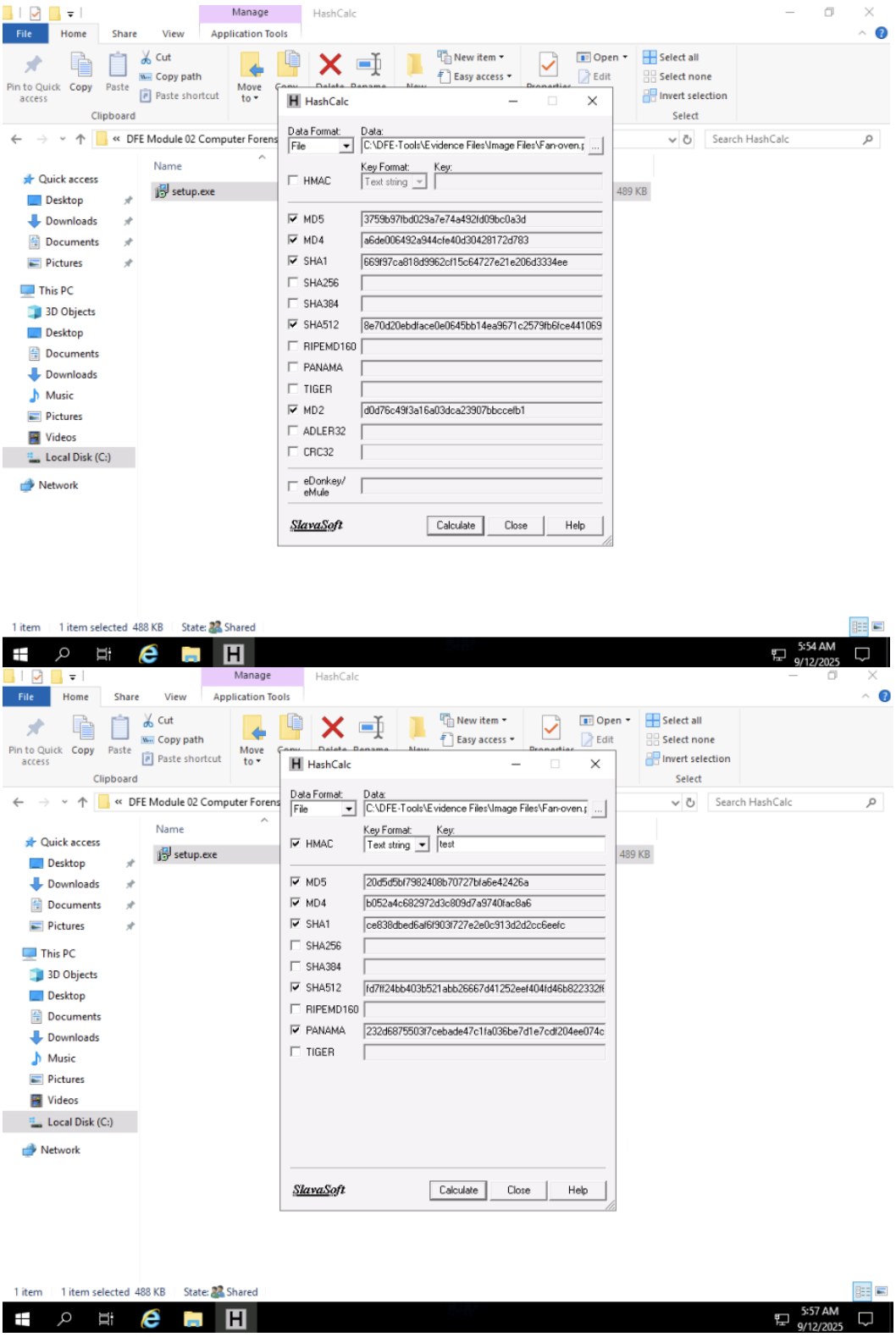
Module 02: Computer Forensics Investigation Process

Lab Scenario:
Cyber-crime incidents are increasing, requiring investigators to follow legal standards and repeatable forensic processes to ensure evidence integrity. This lab introduces the tools and methods used in forensic investigations, including data integrity verification, file analysis, and disk imaging.

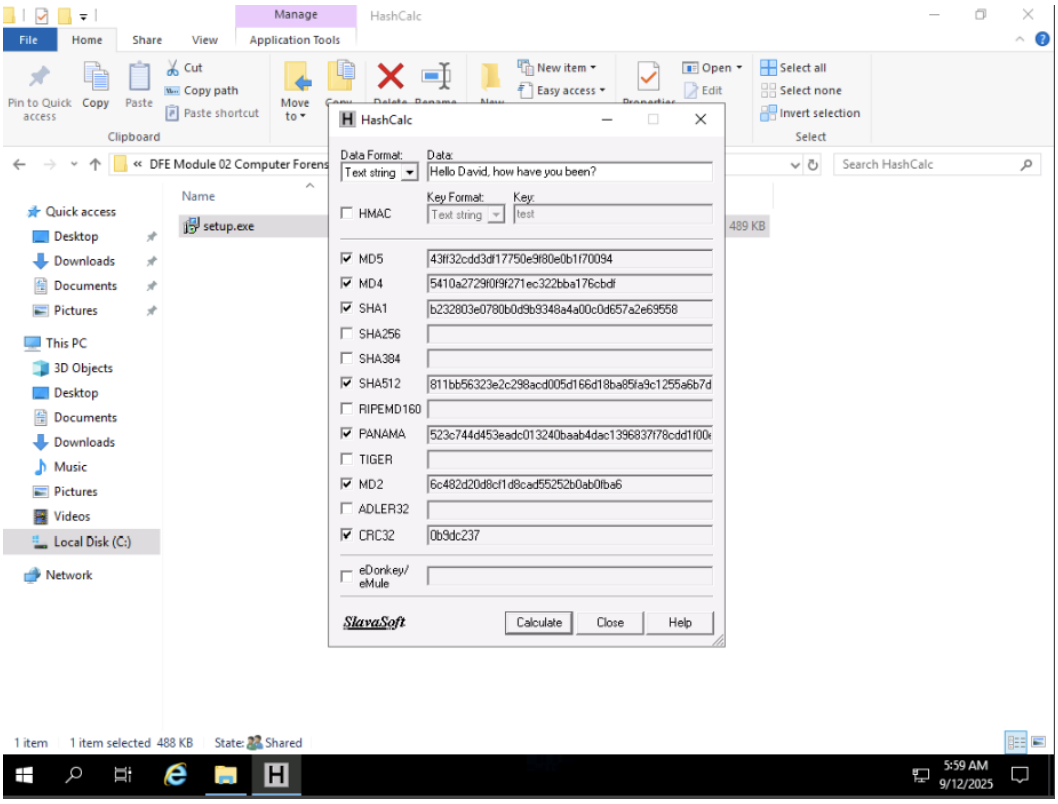
Lab Objectives:
- Generate hashes and checksums to validate data integrity
- Compute MD5 and HMAC values for files and text strings
- Compare hash values to verify file integrity
- Examine files of various formats
- Create forensic disk images of hard disk partitions

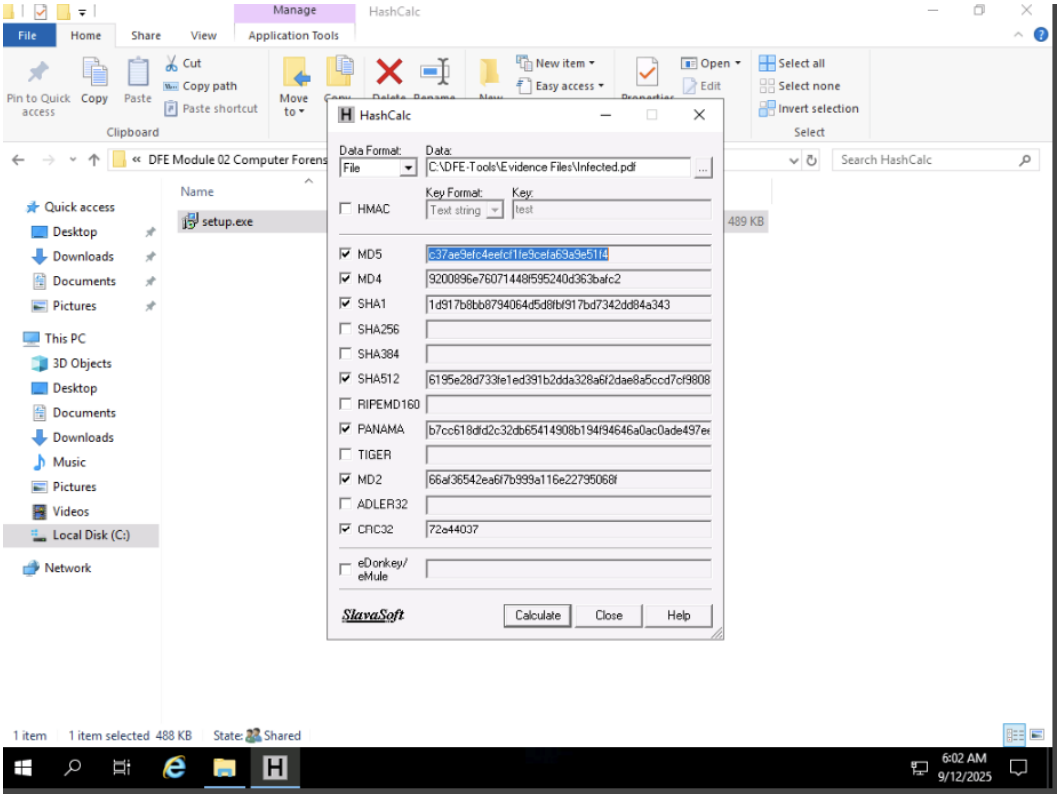
Tools Used:
- HashCalc
- MD5 Calculator
- File Viewer
- R-Drive Image

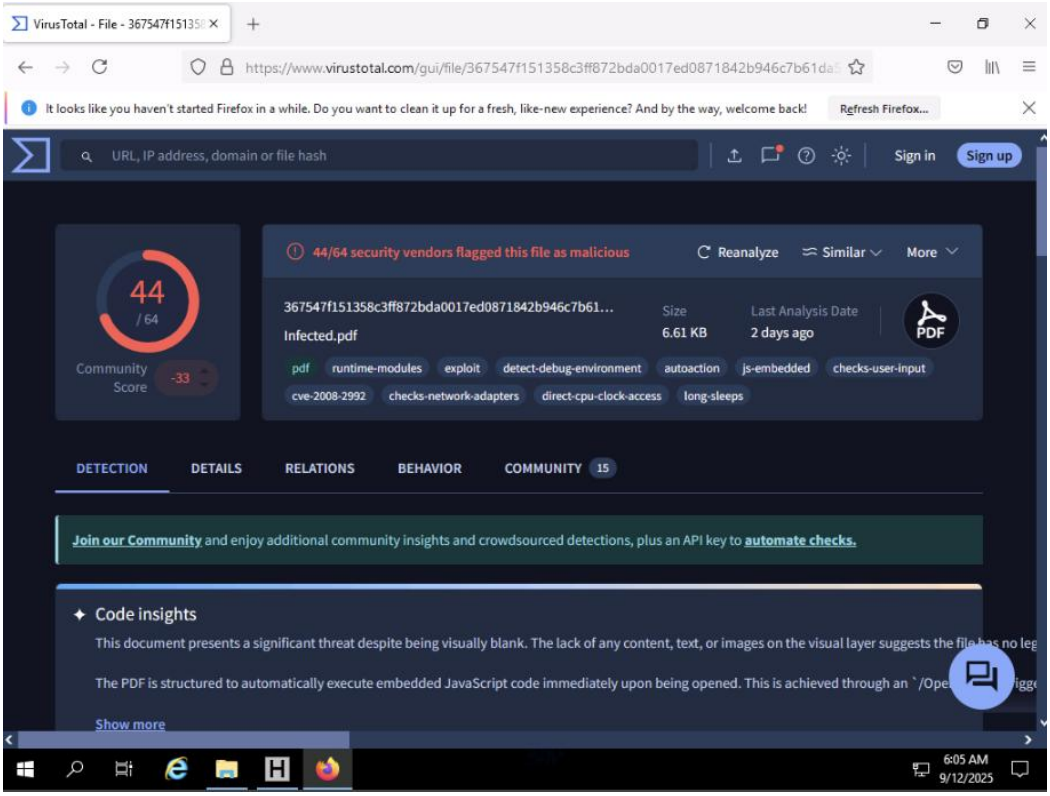
Key Tasks / Methods:
1. **Hash Calculations**
- Calculated file and text string hashes using HashCalc.
- Checked MD5 hash of suspicious files against VirusTotal to assess potential malware.
- Computed HMACs to verify integrity with key strings.

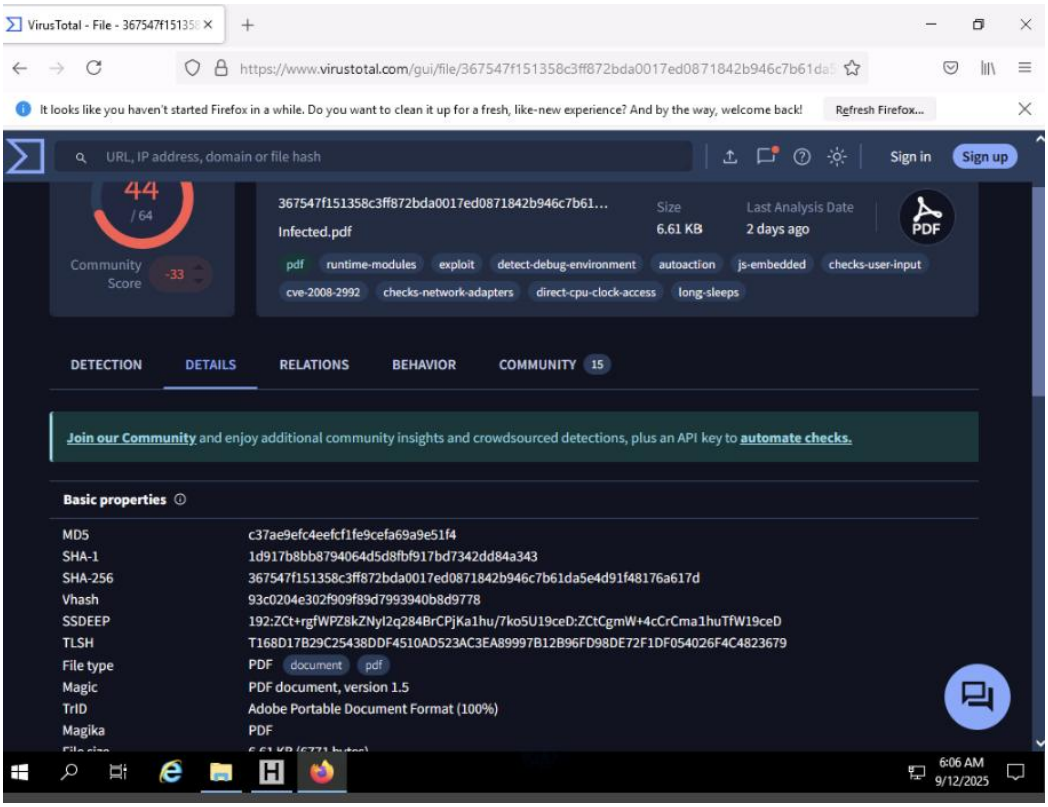


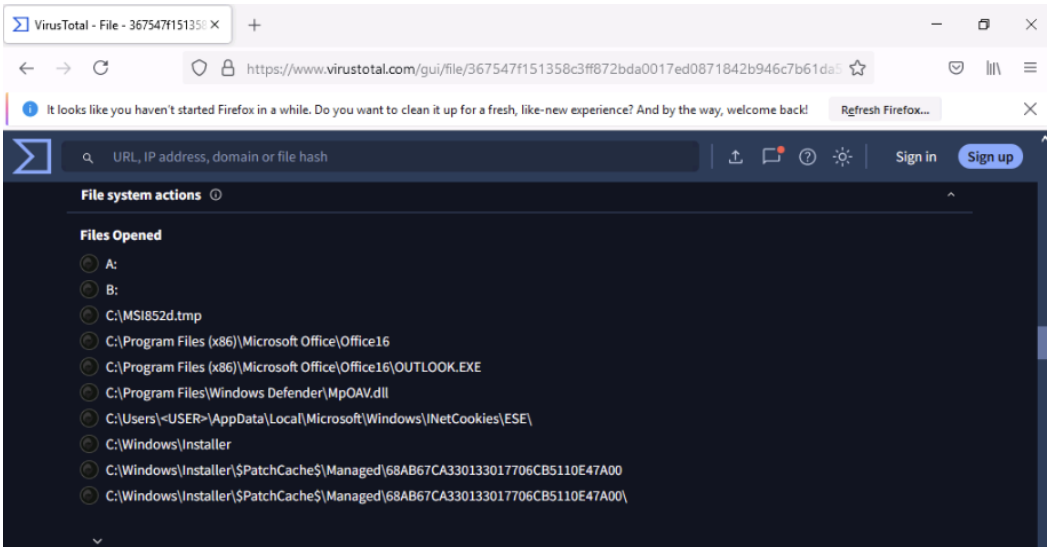
(Screenshot: `Lab2_HashCalc_FanOven.png`)

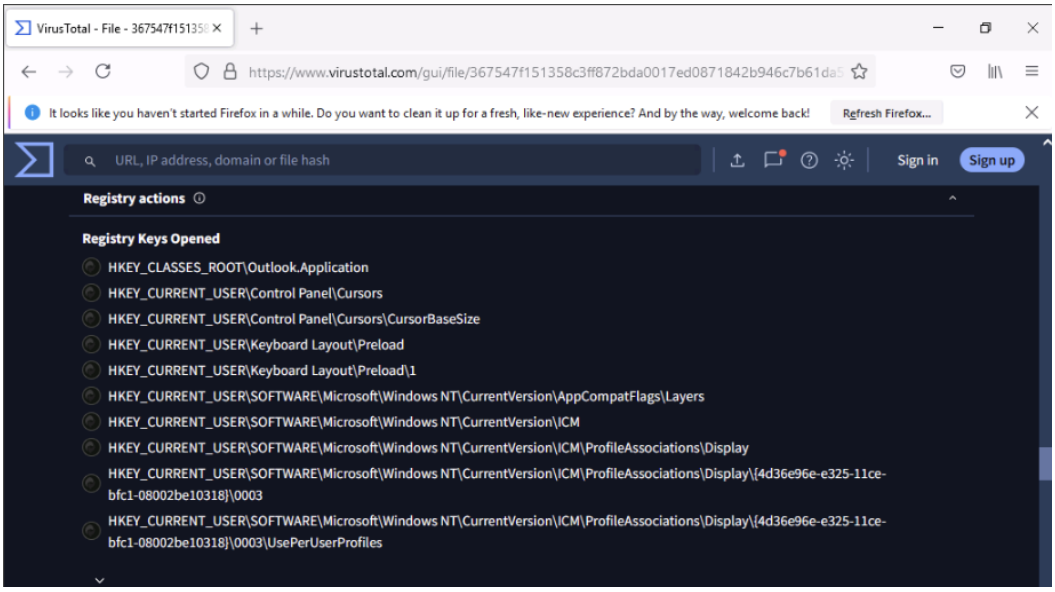

HashCalc
Data Format: Text string
Data: Hello David, how have you been?
Key Format: Text string
Key: test
HMAC
MD5 43ff32cdd3df17750e9f80e0b1f70094
MD4 5410a2729f0f9f271ec322bba176cbdf
SHA1 b232803e0780b0d9b9348a4a00c0d657a2e69558
SHA256
SHA384
SHA512 811bb56323e2c298acd005d166d18ba85fa9c1255a6b7d
RIPEMD160
PANAMA 523c744d453eadc013240baab4dac1396837f78cdd1f00
TIGER
MD2 6c482d20d8cf1d8cad55252b0ab0fba6
ADLER32
CRC32 0b9dc237
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
1 item
1 item selected 488 KB
State: Shared
5:59 AM
9/12/2025

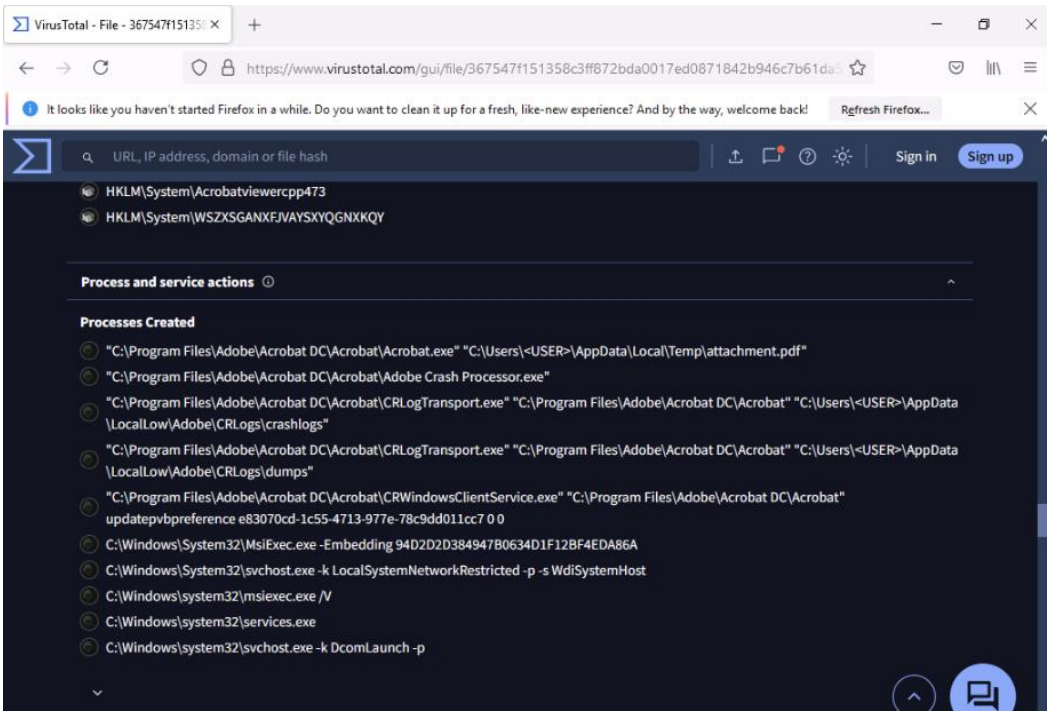

HashCalc
Data Format: File
Data: C:\DFE-Tools\Evidence Files\Infected.pdf
Key Format: Text string
Key: test
HMAC
MD5 c37ae9efc4eefcf1fe9cefa69a9e51f4
MD4 9200896e76071448f595240d363bafc2
SHA1 1d917b8bb8794064d5d8fbf917bd7342dd84a343
SHA256
SHA384
SHA512 6195e28d733fe1ed391b2dda328a6f2dae8a5ccd7cf9808
RIPEMD160
PANAMA b7cc618dfd2c32db65414908b194f94646a0ac0ade497e
TIGER
MD2 66af36542ea6f7b999a116e22795068f
ADLER32
CRC32 72a44037
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
1 item
1 item selected 488 KB
State: Shared
6:02 AM
9/12/2025


VirusTotal - File - 367547f151358
https://www.virustotal.com/gui/file/367547f151358c3ff872bda0017ed0871842b946c7b61da5
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
URL, IP address, domain or file hash
Sign in
Sign up
44
/ 64
Community Score
-33
44/64 security vendors flagged this file as malicious
Reanalyze
Similar
More
367547f151358c3ff872bda0017ed0871842b946c7b61...
Infected.pdf
Size
6.61 KB
Last Analysis Date
2 days ago
PDF
pdf
runtime-modules
exploit
detect-debug-environment
autoaction
js-embedded
checks-user-input
cve-2008-2992
checks-network-adapters
direct-cpu-clock-access
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 15
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Code insights
This document presents a significant threat despite being visually blank. The lack of any content, text, or images on the visual layer suggests the file has no leg
The PDF is structured to automatically execute embedded JavaScript code immediately upon being opened. This is achieved through an `/Ope
Show more
6:05 AM
9/12/2025

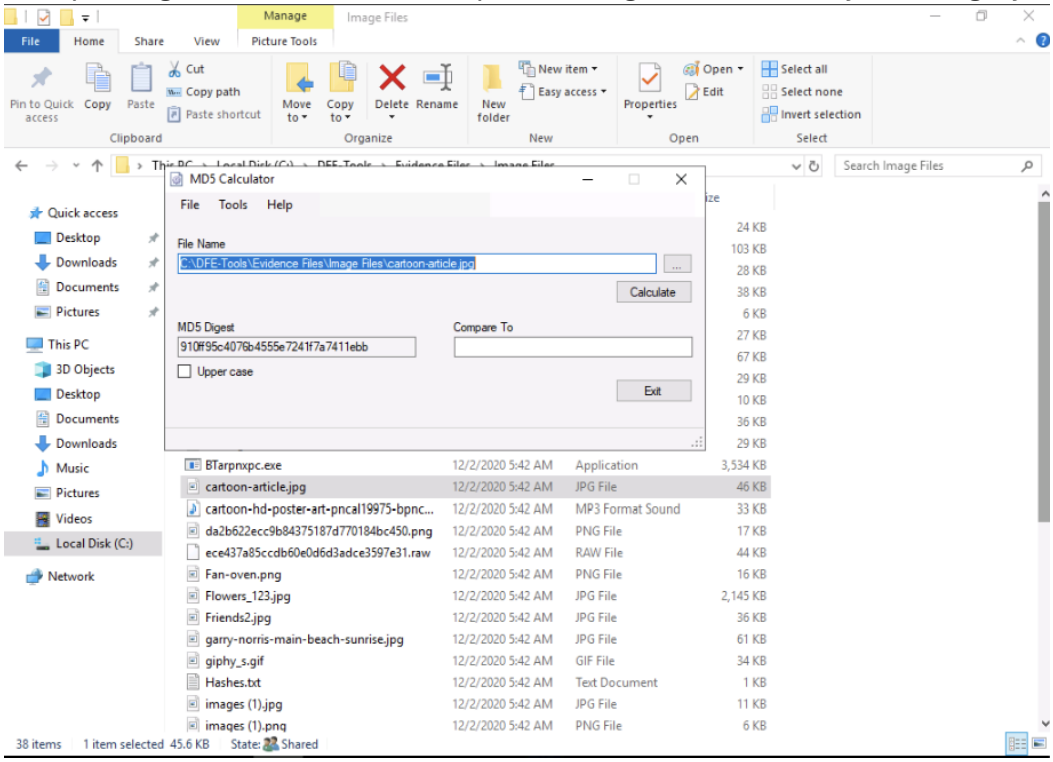

VirusTotal - File - 367547f151358
https://www.virustotal.com/gui/file/367547f151358c3ff872bda0017ed0871842b946c7b61da5
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
URL, IP address, domain or file hash
Sign in
Sign up
44
/ 64
Community Score
-33
367547f151358c3ff872bda0017ed0871842b946c7b61...
Infected.pdf
Size
6.61 KB
Last Analysis Date
2 days ago
PDF
pdf
runtime-modules
exploit
detect-debug-environment
autoaction
js-embedded
checks-user-input
cve-2008-2992
checks-network-adapters
direct-cpu-clock-access
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 15
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 c37ae9efc4eefcf1fe9cefa69a9e51f4
SHA-1 1d917b8bb8794064d5d8fbf917bd7342dd84a343
SHA-256 367547f151358c3ff872bda0017ed0871842b946c7b61da5e4d91f48176a617d
Vhash 93c0204e302f909f89d7993940b8d9778
SSDEEP 192:ZCt+rgfWPZ8kZNyl2q284BrCPjKa1hu/7ko5U19ceD:ZCtCgmW+4cCrCma1huTfW19ceD
TLSH T168D17B29C25438DDF4510AD523AC3EA89997B12B96FD98DE72F1DF054026F4C4823679
File type PDF document pdf
Magic PDF document, version 1.5
TrID Adobe Portable Document Format (100%)
Magika PDF
6:06 AM
9/12/2025

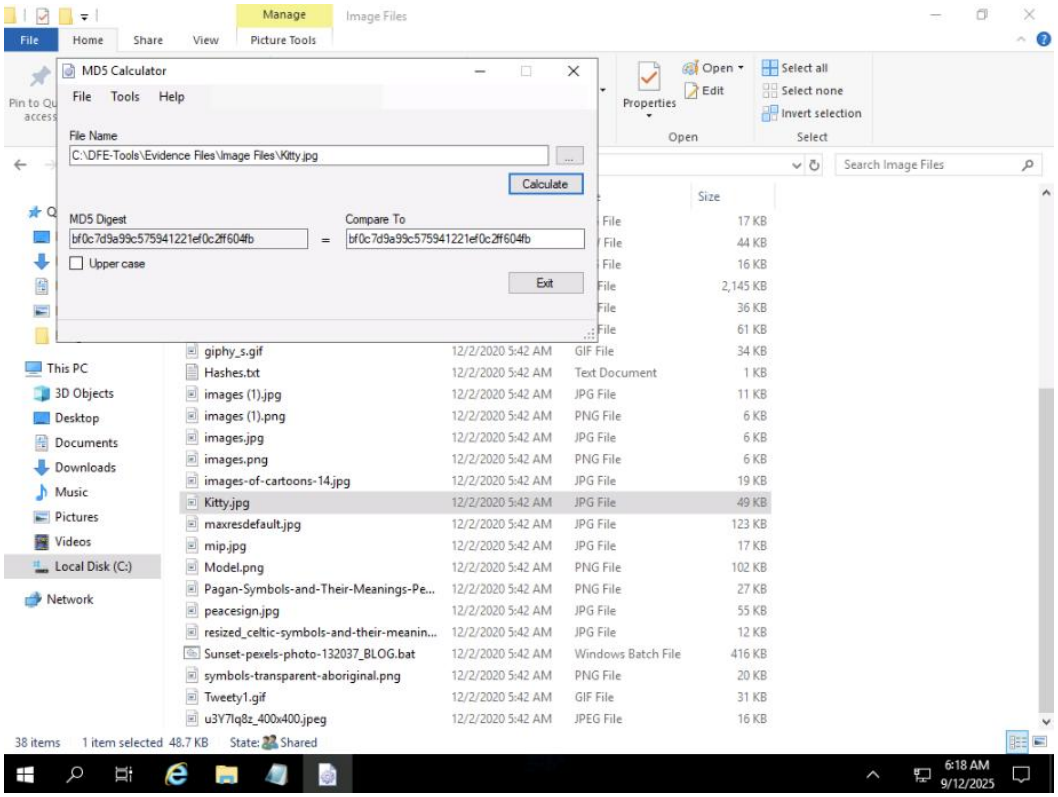

VirusTotal - File - 367547f151358
https://www.virustotal.com/gui/file/367547f151358c3ff872bda0017ed0871842b946c7b61da5
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
URL, IP address, domain or file hash
Sign in
Sign up
File system actions
Files Opened
A:
B:
C:\MSI852d.tmp
C:\Program Files (x86)\Microsoft Office\Office16
C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
C:\Program Files\Windows Defender\MpOAV.dll
C:\Users\<USER>\AppData\Local\Microsoft\Windows\INetCookies\ESE\
C:\Windows\Installer
C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330133017706CB5110E47A00
C:\Windows\Installer\$PatchCache$\Managed\68AB67CA330133017706CB5110E47A00\

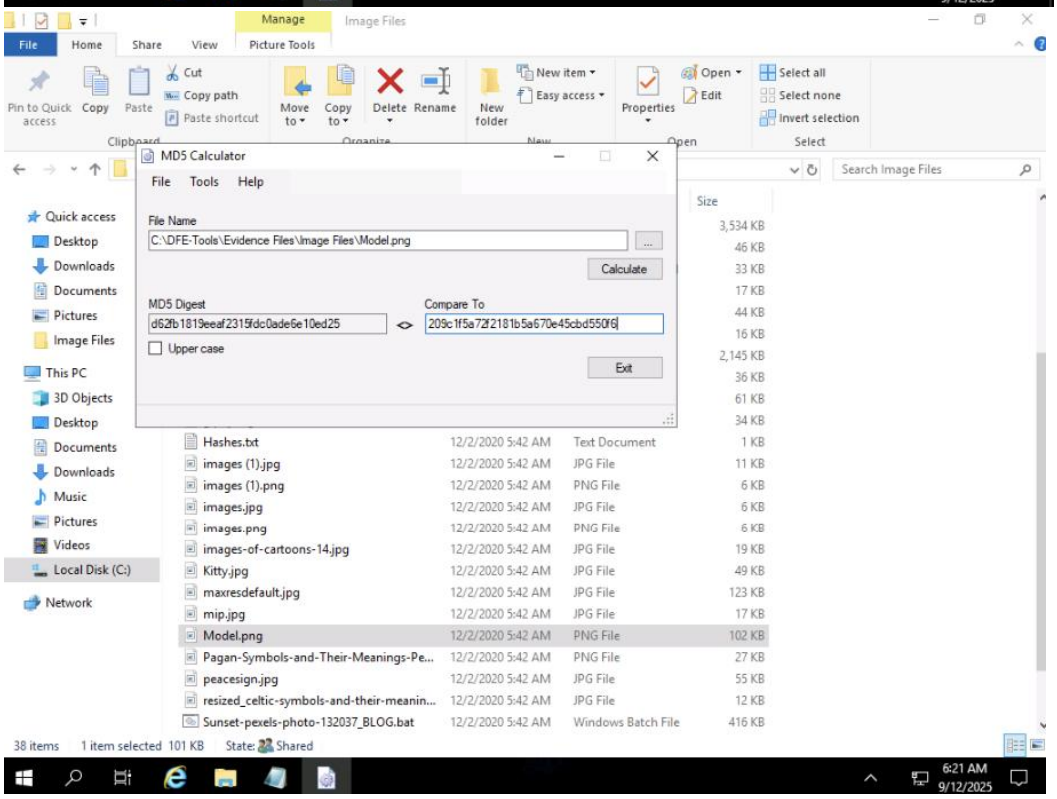

VirusTotal - File - 367547f151358
https://www.virustotal.com/gui/file/367547f151358c3ff872bda0017ed0871842b946c7b61da5
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
URL, IP address, domain or file hash
Sign in
Sign up
Registry actions
Registry Keys Opened
HKEY_CLASSES_ROOT\Outlook.Application
HKEY_CURRENT_USER\Control Panel\Cursors
HKEY_CURRENT_USER\Control Panel\Cursors\CursorBaseSize
HKEY_CURRENT_USER\Keyboard Layout\Preload
HKEY_CURRENT_USER\Keyboard Layout\Preload\1
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ICM
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ICM\ProfileAssociations\Display
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ICM\ProfileAssociations\Display\{4d36e96e-e325-11ce-bfc1-08002be10318}\0003
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ICM\ProfileAssociations\Display\{4d36e96e-e325-11ce-bfc1-08002be10318}\0003\UsePerUserProfiles



2. **Comparing Hash Values**
   - Compared generated hashes with pre-existing hashes to verify file integrity.





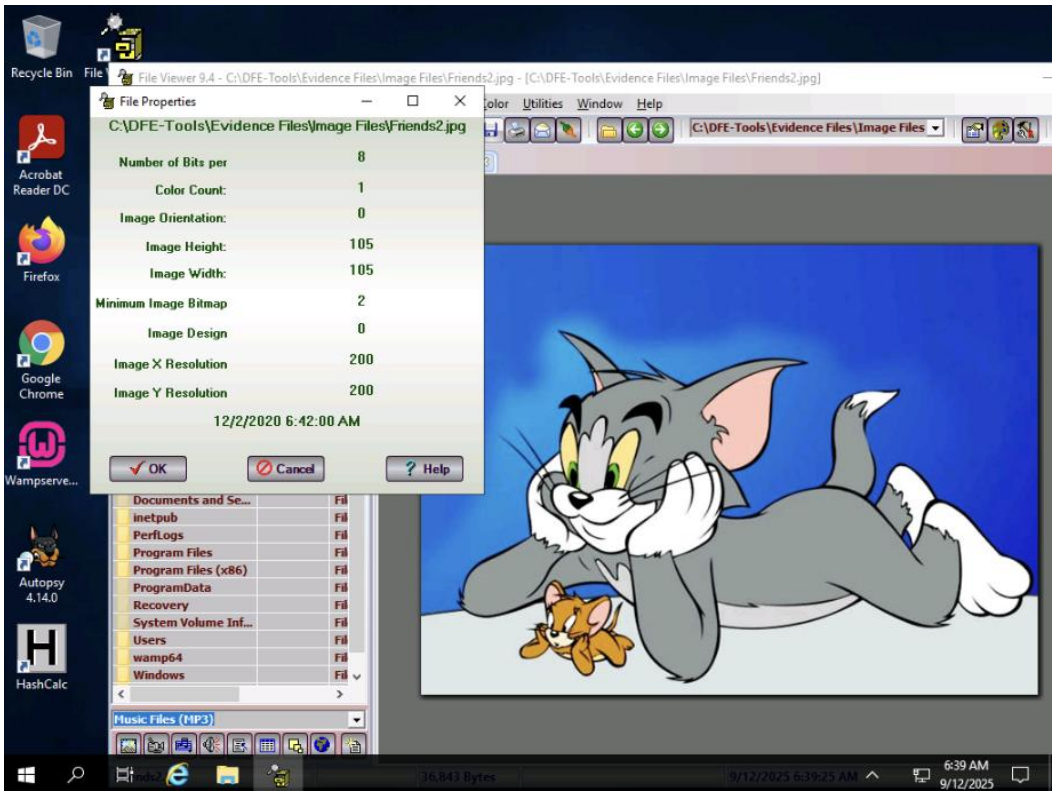


- Identified altered or suspect files requiring further investigation.

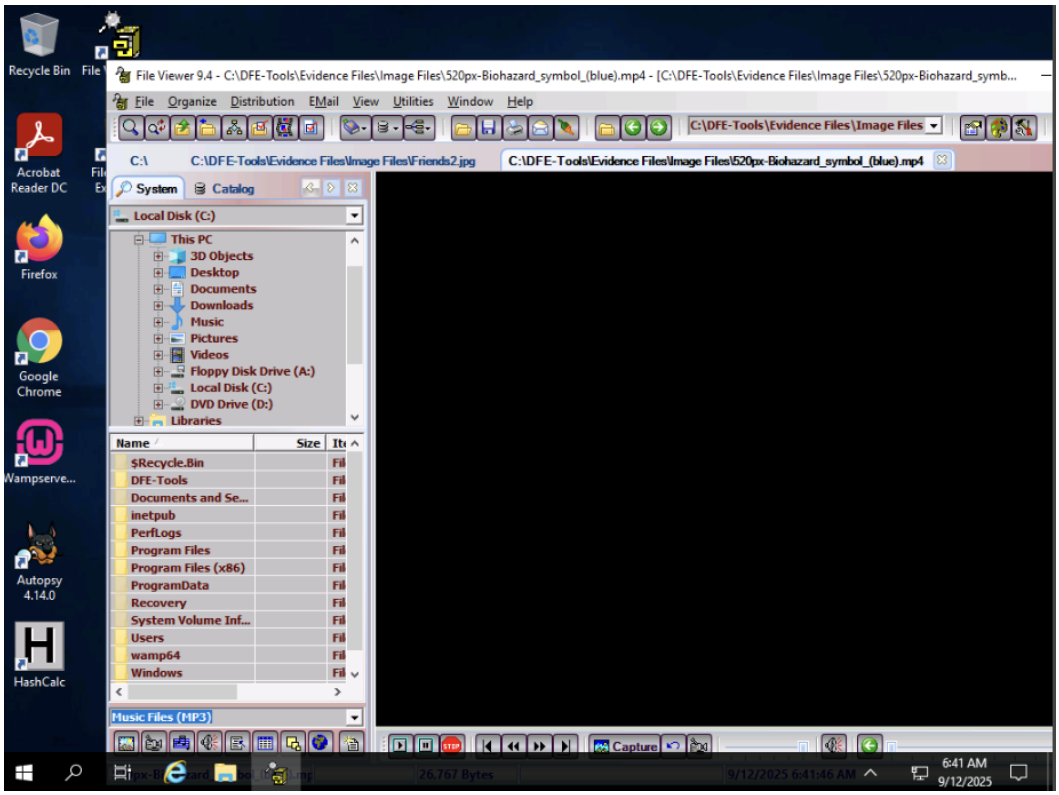
Viewing Files of Various Formats

- Examined images (.jpg), videos (.mp4), and documents using File Viewer.

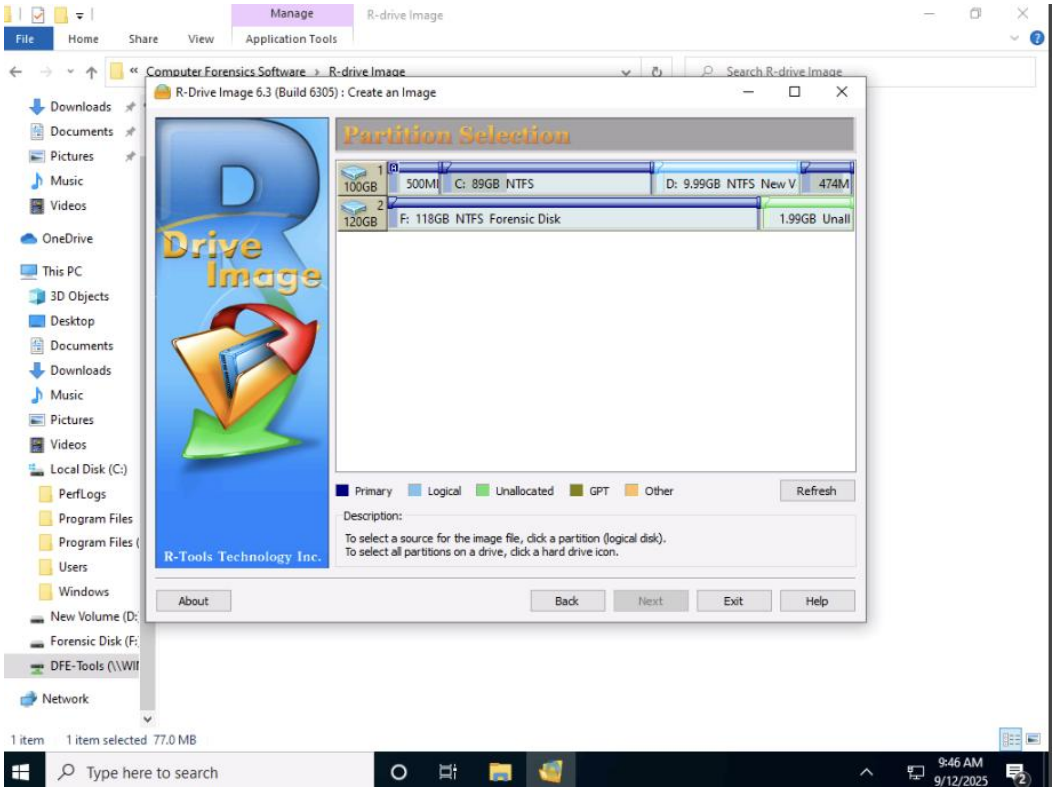
- Determined file type, properties, and potential anomalies for further analysis.

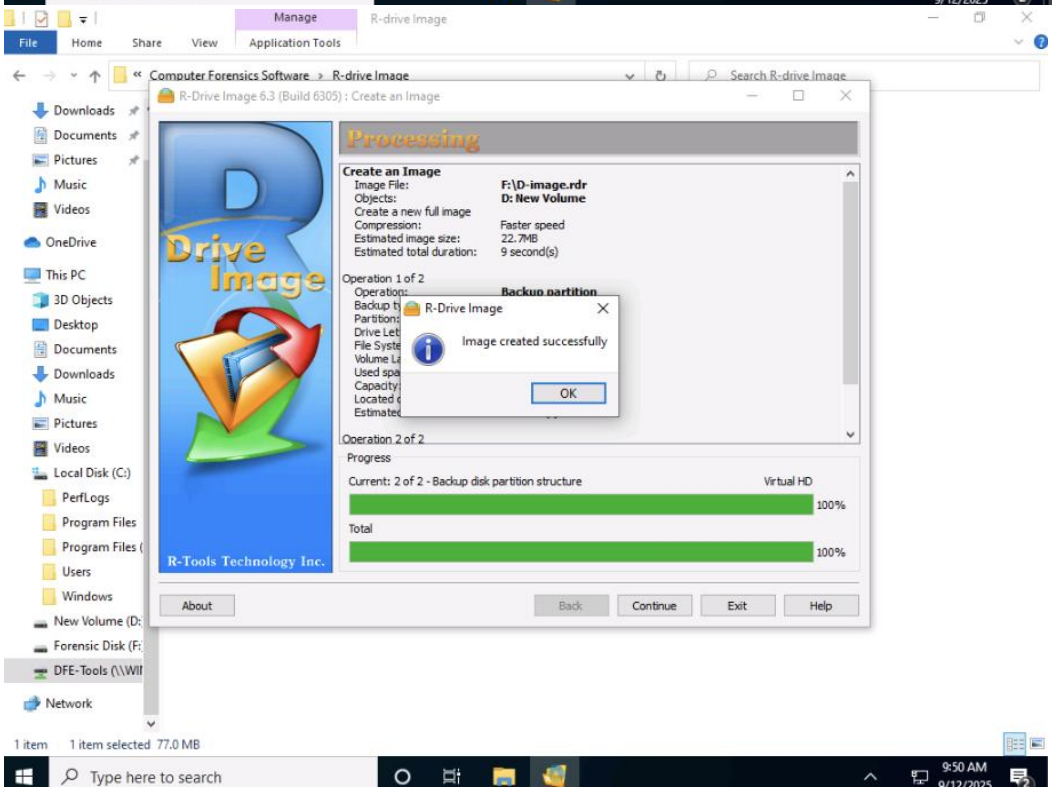


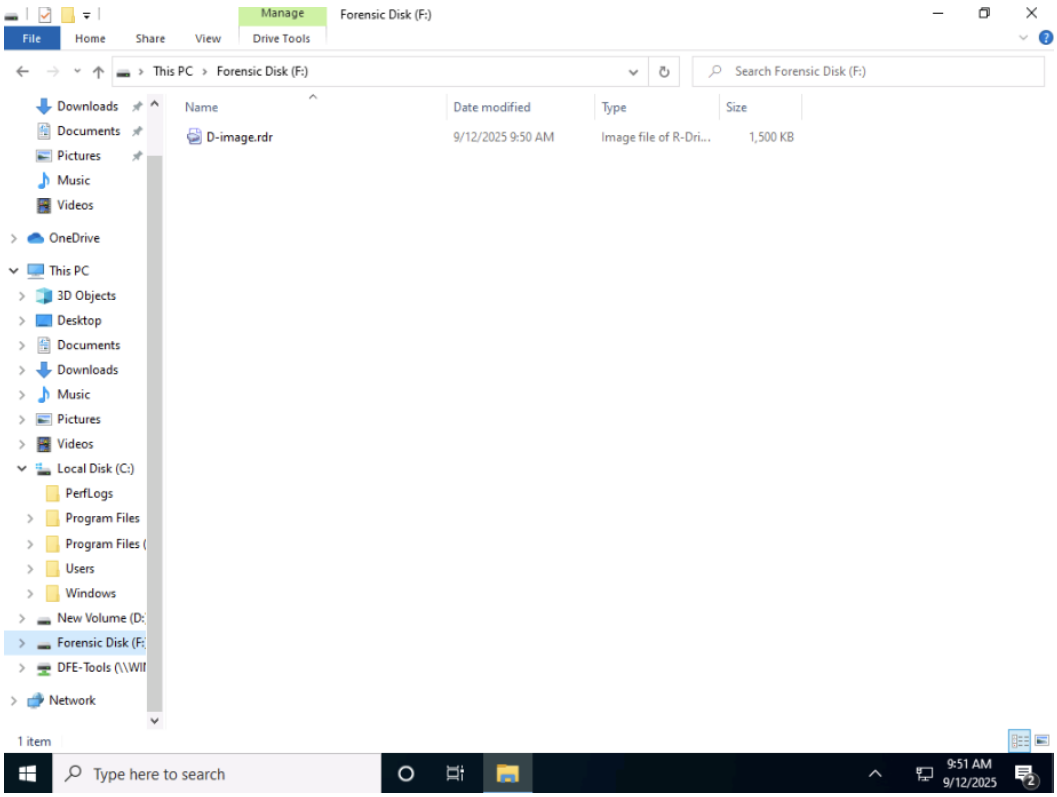
(Screenshot: `Lab2_FileViewer_Friends2.png`)



3. **Creating Disk Images**
    - Created a forensic image of a disk partition using R-Drive Image.
    - Ensured all files, deleted data, and unallocated space were preserved for analysis.


Manage
R-drive Image
File
Home
Share
View
Application Tools
Computer Forensics Software › R-drive Image
Search R-drive Image
R-Drive Image 6.3 (Build 6305) : Create an Image
Partition Selection
1
100GB
500MI
C: 89GB NTFS
D: 9.99GB NTFS New V
474M
2
120GB
F: 118GB NTFS Forensic Disk
1.99GB Unall
Primary
Logical
Unallocated
GPT
Other
Refresh
Description:
To select a source for the image file, click a partition (logical disk).
To select all partitions on a drive, click a hard drive icon.
R-Tools Technology Inc.
About
Back
Next
Exit
Help
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Local Disk (C:)
PerfLogs
Program Files
Users
Windows
New Volume (D:
Forensic Disk (F:
DFE-Tools (\\WI
Network
1 item
1 item selected 77.0 MB
Type here to search
9:46 AM
9/12/2025


Manage
R-drive Image
File
Home
Share
View
Application Tools
Computer Forensics Software › R-drive Image
Search R-drive Image
R-Drive Image 6.3 (Build 6305) : Create an Image
Processing
Create an Image
Image File:
F:\D-image.rdr
Objects:
D: New Volume
Create a new full image
Compression:
Faster speed
Estimated image size:
22.7MB
Estimated total duration:
9 second(s)
Operation 1 of 2
Backup partition
R-Drive Image
Image created successfully
OK
Operation 2 of 2
Progress
Current: 2 of 2 - Backup disk partition structure
Virtual HD
100%
Total
100%
R-Tools Technology Inc.
About
Back
Continue
Exit
Help
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Local Disk (C:)
PerfLogs
Program Files
Users
Windows
New Volume (D:
Forensic Disk (F:
DFE-Tools (\\WI
Network
1 item
1 item selected 77.0 MB
Type here to search
9:50 AM



(Screenshot: `Lab2_RDriveImage_DPartition.png`)

Outcome / Personal Reflection:

This lab provided practical experience with core forensic tools and processes. I gained hands-on skills in validating digital evidence, analyzing different file formats, and creating forensic disk images, all crucial for real-world computer forensic investigations.