

CS 4241  
**CYBER FORENSICS**  
**LAB REPORTS**

By G Shalom  
BT19GCS004

## Table Of Contents

S.No	Date	Report	Page No
1	3/8/22	Volatility	3
2	31/8/22	Wireshark & Autopsy	7
3	21/9/22	EXIF Tool	15
4	28/9/22	BruteShark & LiveForensicator	18
5	2/11/22	WinHex	24
6	9/11/22	Browser Forensics	27
7	23/11/22	Container Forensics	29

## Lab Assignment 1

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 1
- 4. Title of the Program/Experiment:** Memory Forensics
- 5. Date Program/Experiment Performed:** 10/08/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To analyze memory dump files using volatility tool

**8. Description:**

**a. Overview**

We have to analyze memory dump files to do memory forensics using volatility tool.

**b. System Requirement: (Software and Hardware)**

- Python version 2.6 or later
- A Windows, Linux, or Mac OS X machine
- Distorm3 for analysis of 64-bit Windows
- Git
- Volatility tool
- DumpIt tool

**c. Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

**d. Algorithm (Step by Step Approach)**

No algorithms were used

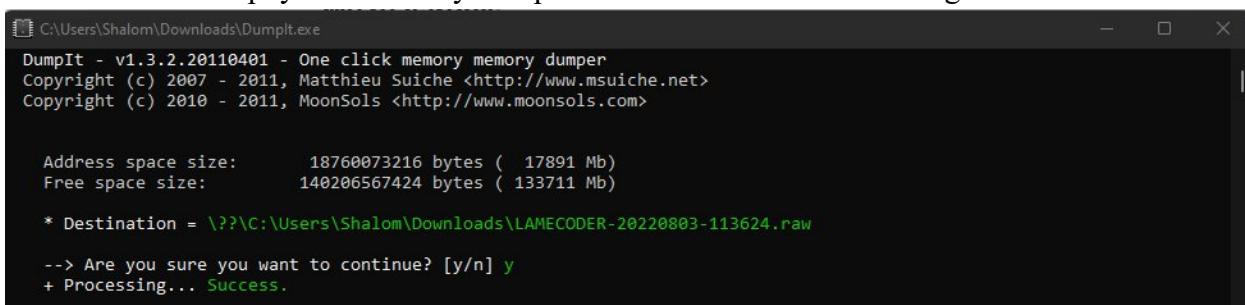
**9. Implementation Details:**

**a. In case of programming implementation: Please add source code**

No programming was done.

**b. In case of software installation: Please add screenshots. (Step by Step)**

DumpIt tool (from <https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt>) was downloaded to create a raw memory dump. The tool was run and a physical memory dump of the Windows machine was generated.



```

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      18760073216 bytes ( 17891 Mb)
Free space size:        140206567424 bytes ( 133711 Mb)

* Destination = \??\C:\Users\Shalom\Downloads\LAMECODER-20220803-113624.raw

--> Are you sure you want to continue? [y/n] y
+ Processing... Success.

```

Volatility tool (<https://github.com/volatilityfoundation/volatility3>) was downloaded .

Run vol.py to check if it is working fine or not.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py
Volatility 3 Framework 2.0.1
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off{}}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION]
                  [--stackers [$STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: Please select a plugin to run
```

Run various commands to gain intel.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.pslist
Volatility 3 Framework 2.0.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName  Offset(V)    Threads Handles SessionId    Wow64  CreateTime     ExitTime      File output
4      0       System       0x823c89c8  53        240    N/A    False    N/A    Disabled
368    4       smss.exe     0x822f1020  3         19    N/A    False    2012-07-22 02:42:31.000000  N/A    Disabled
584    368    csrss.exe    0x822a0598  9         326    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
608    368    winlogon.exe 0x82298700  23        519    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
652    608    services.exe 0x81e2ab28  16        243    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
664    608    lsass.exe    0x81e2a3b8  24        330    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
824    652    svchost.exe  0x82311360  20        194    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
908    652    svchost.exe  0x81e29ab8  9         226    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
1004   652    svchost.exe  0x823001d0  64        1118   0     False    2012-07-22 02:42:33.000000  N/A    Disabled
1056   652    svchost.exe  0x821dfda0  5         60    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
1220   652    svchost.exe  0x82295650  15        197    0     False    2012-07-22 02:42:35.000000  N/A    Disabled
1484   1464   explorer.exe 0x821dea70  17        415    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
1512   652    spoolsv.exe 0x81eb17b8  14        113    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
1640   1484   reader_sl.exe 0x81e7bda0  5         39    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
788    652    alg.exe     0x820e8da0  7         104    0     False    2012-07-22 02:43:01.000000  N/A    Disabled
1136   1004   wuauctl.exe 0x821fcda0  8         173    0     False    2012-07-22 02:43:46.000000  N/A    Disabled
1588   1004   wuauctl.exe 0x8205bda0  5         132    0     False    2012-07-22 02:44:01.000000  N/A    Disabled
```

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.pstree
Volatility 3 Framework 2.0.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName  Offset(V)    Threads Handles SessionId    Wow64  CreateTime     ExitTime
4      0       System       0x823c89c8  53        240    N/A    False    N/A
* 368    4       smss.exe     0x822f1020  3         19    N/A    False    2012-07-22 02:42:31.000000  N/A
** 584    368    csrss.exe    0x822a0598  9         326    0     False    2012-07-22 02:42:32.000000  N/A
** 608    368    winlogon.exe 0x82298700  23        519    0     False    2012-07-22 02:42:32.000000  N/A
*** 664    608    lsass.exe    0x81e2a3b8  24        330    0     False    2012-07-22 02:42:32.000000  N/A
*** 652    608    services.exe 0x81e2ab28  16        243    0     False    2012-07-22 02:42:32.000000  N/A
**** 1056   652    svchost.exe  0x821dfda0  5         60    0     False    2012-07-22 02:42:33.000000  N/A
**** 1220   652    svchost.exe  0x82295650  15        197    0     False    2012-07-22 02:42:35.000000  N/A
**** 1512   652    spoolsv.exe 0x81eb17b8  14        113    0     False    2012-07-22 02:42:36.000000  N/A
**** 908    652    svchost.exe  0x81e29ab8  9         226    0     False    2012-07-22 02:42:33.000000  N/A
**** 1004   652    svchost.exe  0x823001d0  64        1118   0     False    2012-07-22 02:42:33.000000  N/A
**** 1136   1004   wuauctl.exe 0x821fcda0  8         173    0     False    2012-07-22 02:43:46.000000  N/A
**** 1588   1004   wuauctl.exe 0x8205bda0  5         132    0     False    2012-07-22 02:44:01.000000  N/A
**** 788    652    alg.exe     0x820e8da0  7         104    0     False    2012-07-22 02:43:01.000000  N/A
**** 824    652    svchost.exe  0x82311360  20        194    0     False    2012-07-22 02:42:33.000000  N/A
* 1484   1464   explorer.exe 0x821dea70  17        415    0     False    2012-07-22 02:42:36.000000  N/A
* 1640   1484   reader_sl.exe 0x81e7bda0  5         39    0     False    2012-07-22 02:42:36.000000  N/A
```

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.psscan
Volatility 3 Framework 2.0.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName  Offset(V)    Threads Handles SessionId    Wow64  CreateTime     ExitTime      File output
908    652    svchost.exe  0x2029ab8  9         226    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
664    608    lsass.exe    0x202a3b8  24        330    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
652    608    services.exe 0x202ab28  16        243    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
1640   1484   reader_sl.exe 0x207bda0  5         39    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
1512   652    spoolsv.exe 0x20b17b8  14        113    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
1588   1004   wuauctl.exe 0x225bda0  5         132    0     False    2012-07-22 02:44:01.000000  N/A    Disabled
788    652    alg.exe     0x22e8da0  7         104    0     False    2012-07-22 02:43:01.000000  N/A    Disabled
1484   1464   explorer.exe 0x23dea70  17        415    0     False    2012-07-22 02:42:36.000000  N/A    Disabled
1056   652    svchost.exe  0x23dfda0  5         60    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
1136   1004   wuauctl.exe 0x23fcda0  8         173    0     False    2012-07-22 02:43:46.000000  N/A    Disabled
1220   652    svchost.exe  0x2495650  15        197    0     False    2012-07-22 02:42:35.000000  N/A    Disabled
608    368    winlogon.exe 0x2498700  23        519    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
584    368    csrss.exe    0x24a0598  9         326    0     False    2012-07-22 02:42:32.000000  N/A    Disabled
368    4       smss.exe     0x24f1020  3         19    N/A    False    2012-07-22 02:42:31.000000  N/A    Disabled
1004   652    svchost.exe  0x25001d0  64        1118   0     False    2012-07-22 02:42:33.000000  N/A    Disabled
824    652    svchost.exe  0x2511360  20        194    0     False    2012-07-22 02:42:33.000000  N/A    Disabled
4      0       System       0x252c89c8  53        240    N/A    False    N/A    Disabled
```

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.netscan
Volatility 3 Framework 2.0.1
Progress: 100.00          PDB scanning finished
Offset Proto LocalAddr LocalPort ForeignAddr ForeignPort State PID Owner Created
Traceback (most recent call last):
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\vol.py", line 10, in <module>
    volatility3.cli.main()
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\__init__.py", line 625, in main
    Commandline().run()
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\__init__.py", line 333, in run
    renderers[args.renderer()].render(constructed.run())
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\text_renderer.py", line 178, in render
    grid.populate(visitor, outfd)
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3\framework\renderers\__init__.py", line 212, in populate
    for (level, item) in self._generator:
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 282, in _generator
    netscan_symbol_table = self.create_netscan_symbol_table(self.context, kernel.layer_name,
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 238, in create_netscan_symbol_table
    symbol_filename, class_types = cls.determine_tcpip_version(
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 215, in determine_tcpip_version
    raise NotImplementedError("This version of Windows is not supported: {}.{}.{!}.".format(
  NotImplementedError: This version of Windows is not supported: 5.1 15.2600!
```

## 10. Error Description:

1. Getting all required libraries wasn't possible due to errors in installing snappy library. Also found a link for possible fix

(<https://stackoverflow.com/questions/42979544/how-to-install-snappy-c-libraries-on-windows-10-for-use-with-python-snappy-in-an>) but it resulted in another error, which wasn't fixable.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> pip3 install -r requirements.txt
Requirement already satisfied: pefile>=2017.8.1 in c:\users\shalom\appdata\local\programs\python\python310\lib\site-packages (from -r requirements.txt (line 2)) (2022.5.30)
Collecting yara-python>=3.8.0
  Downloading yara_python-4.2.0-cp310-cp310-win_amd64.whl (1.1 MB)
    1.1/1.1 MB 1.7 MB/s eta 0:00:00
Collecting capstone>=3.0.5
  Downloading capstone-4.0.2-py2.py3-none-win_amd64.whl (896 kB)
    896.4/896.4 KB 2.2 MB/s eta 0:00:00
Collecting pycryptodome
  Downloading pycryptodome-3.15.0-cp35-abi3-win_amd64.whl (1.9 MB)
    1.9/1.9 MB 1.9 MB/s eta 0:00:00
Collecting jsonschema>=2.3.0
  Downloading jsonschema-4.9.1-py3-none-any.whl (79 kB)
    79.5/79.5 KB 2.2 MB/s eta 0:00:00
Collecting leechcorepyc>=2.4.8
  Downloading leechcorepyc-2.12.0-cp36-abi3-win_amd64.whl (347 kB)
    347.2/347.2 KB 2.2 MB/s eta 0:00:00
Collecting python-snappy>=0.6.8
  Downloading python-snappy-0.6.8.tar.gz (21 kB)
  Preparing metadata (setup.py) ... done
Requirement already satisfied: future in c:\users\shalom\appdata\local\programs\python\python310\lib\site-packages (from pefile>=2017.8.1->-r requirements.txt (line 2)) (0.18.2)
Collecting pyrsistent<0.17.0,>=0.17.1,<0.17.2,>=0.14.0
  Downloading pyrsistent-0.18.1-cp310-cp310-win_amd64.whl (61 kB)
    61.6/61.6 KB 3.4 MB/s eta 0:00:00
Collecting attrs>=17.4.0
  Downloading attrs-22.1.0-py2.py3-none-any.whl (58 kB)
    58.8/58.8 KB 3.2 MB/s eta 0:00:00
using legacy 'setup.py install' for python-snappy, since package 'wheel' is not installed.
Installing collected packages: yara-python, python-snappy, pyrsistent, pycryptodome, leechcorepyc, capstone, attrs, jsonschema
  Running setup.py install for python-snappy ... error
    error: subprocess-exited-with-error

      × Running setup.py install for python-snappy did not run successfully.
      | exit code: 1
      | [26 lines of output]
      |   C:\Users\Shalom\AppData\Local\Programs\Python\Python310\lib\distutils\dist.py:274: UserWarning: Unknown distribution option: 'ccffi_modules'
      |     warnings.warn(msg)
      |
      |   running install
      |   running build
      |   running build_py
      |   creating build
      |   creating build\lib.win-amd64-3.10
      |   creating build\lib.win-amd64-3.10\snappy
      |   copying snappy\hadoop_snappy.py --> build\lib.win-amd64-3.10\snappy
      |   copying snappy\snappy.py --> build\lib.win-amd64-3.10\snappy
      |   copying snappy\snappy_cffi.py --> build\lib.win-amd64-3.10\snappy
      |   copying snappy\snappy_cffi.builder.py --> build\lib.win-amd64-3.10\snappy
      |   copying snappy\snappy_formats.py --> build\lib.win-amd64-3.10\snappy
      |   copying snappy\__init__.py --> build\lib.win-amd64-3.10\snappy
      |
      |   volatility3.cll: The following programs will be loaded by volatility3 to see why: volatility3.plugins.windows_pslist
      |   INFO: volatility3.framework: Loaded a programemory plugin
      |   INFO: volatility3.framework: Running automatic: ConstructionMagic
      |   INFO: volatility3.framework.automatic: Running automatic: LayerStacker
      |   DEBUG: volatility3.framework.automatic.windows: Self-referential pointer for recent windows
      |   DEBUG: volatility3.framework.automatic.windows: Detected self-referential pointer at 0x1ae000
      |   DEBUG: volatility3.framework.automatic.windows: DTB was found at 0x1ae000
      |   DEBUG: volatility3.framework.automatic.windows: DTB was found at 0x1ae000
      |   DEBUG: volatility3.framework.automatic.stacker: Stacked layers: ['IntellLayer', 'FileLayer']
      |   INFO: volatility3.framework.automatic: Running automatic: WinMapScanner
      |   INFO: volatility3.framework.automatic: Running automatic: KernelOBScanner
      |   DEBUG: volatility3.framework.automatic.pdbscan: Kernel base determination - searching layer module list structure
      |   DEBUG: volatility3.framework.automatic.pdbscan: Setting kernel_virtual_offset to 0x80770800000
      |   DEBUG: volatility3.framework.symbols.windows.pdbutil: Using symbol library: ntkrnlap.dll!0E373D0612E747F0E72EF02E67083-1
      |   INFO: volatility3.framework.schemas: All schemas validated
      |   DEBUG: volatility3.schemas: All validations will report success, even with malformed input
      |   INFO: volatility3.framework.automatic: Running automatic: KernelModule
      |
      PID  P0ID ImageFileHandle  Offset(V)  Threads Handler SessionId  Wow64  CreateTime  ExitTime  File output
INFO: volatility3.schemas: Dependency for validation unavailable: jsonschema
DEBUG: volatility3.schemas: All validations will report success, even with malformed input
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_PO_PROCESS_ENERGY_CONTEXT
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_EPROCESS_VOTA_BLOCK
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_VOLATILITY_VOTA_BLOCK
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!PAGEFAULT_HISTORY
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!JOB_ACCESS5_STATE
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!JOB_CPU_RATE_CONTROL
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!JOB_NOTIFICATION_INFORMATION
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!PSP_STORAGE
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!ACTIVATION_CONTEXT_DATA
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_ASSEMBLY_STORAGE_MAP
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_EXP_LICENSE_STATE
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_NLS_STATE
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_DBGP_ERROR_PORT
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_FILE_SYSTEM_PATHS
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_EX_WNF_SUBSCRIPTION
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_ETW_EVENT_CALLBACK_CONTEXT
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_ETW_SOFT_RESTART_CONTEXT
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_FILE_SELECT_HASH_FUNCTION
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_EX_TIMER
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_HAL_PMC_COUNTERS
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_IORING_OBJECT
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_DEVICE_NODE_IOMMU_EXTENSION
DEBUG: volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_SCSI_REQUEST_BLOCK
```

2. Invalid process detected in the memory dump created of Windows 11, possible system issue as Windows XP dump ran fine.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\vol.py -vv -f "C:\Users\Shalom\Downloads\LAEMECODER-20220803-113624.raw" windows_pslist
Volatility 3 Framework 2.0.1
  ...
  Volatility3 framework: Volatility plugins path: 'C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility\plugins', 'C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility\symbols', 'C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility\framework\plugins\windows'
INFO: volatility3.framework.volatility: Volatility symbols path: 'C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility\framework\plugins\windows\symbols'
DEBUG: volatility3.framework: No module named 'Crypto'
DEBUG: volatility3.framework: Failed to import module volatility3.plugins.windows.cacheandump based on file: C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3\framework\plugins\windows\cacheandump.py
DEBUG: volatility3.framework: Failed to import module volatility3.plugins.windows.hashdump based on file: C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3\framework\plugins\windows\hashdump.py
DEBUG: volatility3.framework: Failed to import module volatility3.plugins.windows.lsadump based on file: C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3\framework\plugins\windows\lsadump.py
INFO: volatility3.framework: The following programs will be loaded by volatility3 to see why: volatility3.plugins.windows_pslist
INFO: volatility3.framework: Loaded a programemory plugin
INFO: volatility3.framework.automatic: Running automatic: ConstructionMagic
INFO: volatility3.framework.automatic: Running automatic: LayerStacker
DEBUG: volatility3.framework.automatic.windows: Self-referential pointer for recent windows
DEBUG: volatility3.framework.automatic.windows: Detected self-referential pointer at 0x1ae000
DEBUG: volatility3.framework.automatic.windows: DTB was found at 0x1ae000
DEBUG: volatility3.framework.automatic.stackers: Stacked layers: ['IntellLayer', 'FileLayer']
INFO: volatility3.framework.automatic: Running automatic: WinMapScanner
INFO: volatility3.framework.automatic: Running automatic: KernelOBScanner
DEBUG: volatility3.framework.automatic.pdbscan: Kernel base determination - searching layer module list structure
DEBUG: volatility3.framework.automatic.pdbscan: Setting kernel_virtual_offset to 0x80770800000
DEBUG: volatility3.framework.symbols.windows.pdbutil: Using symbol library: ntkrnlap.dll!0E373D0612E747F0E72EF02E67083-1
INFO: volatility3.framework.schemas: All validations will report success, even with malformed input
DEBUG: volatility3.framework.automatic: Running automatic: KernelModule
INFO: volatility3.plugins.windows_pslist: Invalid process found at address: e5e5e5e5e19d. Skipping
```

3. Windows Kernel error when tried to analyze memory dumps created automatically by Windows

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1> py vol.py -v -f "C:\Users\Shalom\Desktop\880522-10359-01.dmp" windows.psscan
Volatility 3 Framework 2.0.1
INFO volatility3.cli: Volatility plugins path: ['C:\\Users\\Shalom\\Downloads\\\\volatility3-2.0.1\\\\volatility3\\plugins', 'C:\\Users\\Shalom\\Downloads\\volatility3-2.0.1\\\\volatility3-2.0.1\\\\volatility3\\symbols']
INFO volatility3.cli: Volatility symbols path: ['C:\\Users\\Shalom\\Downloads\\\\volatility3-2.0.1\\\\volatility3\\symbols', 'C:\\Users\\Shalom\\Downloads\\volatility3-2.0.1\\\\volatility3-2.0.1\\\\volatility3\\symbols']
INFO volatility3.cli: The following plugins could not be loaded (use -vv to see why): volatility3.plugins.windows.cachedump, volatility3.plugins.windows.hashdump, volatility3.plugins.windows.lsadump
INFO volatility3.framework.automatic: Detected a windows category plugin
INFO volatility3.framework.automatic: Running automatic: ConstructionMagic
INFO volatility3.framework.automatic: Running automatic: LayerStacker
INFO volatility3.schemas: Dependency for validation unavailable: jsonschema
INFO volatility3.schemas: Dependency for validation unavailable: jsonschema
INFO volatility3.framework.automatic: Running automatic: WinMapPlayers
INFO volatility3.framework.automatic: Running automatic: KernelPOBScanner
INFO volatility3.framework.automatic: No suitable kernels found during pdbscan
INFO volatility3.framework.automatic: Running automatic: KernelModule

unsatisfied requirement.plugins.PsScan.kernel: Windows kernel
unable to validate the plugin requirements: ['plugins.PsScan.kernel']

Tried getting a profile but was not able to detect kernel
```

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1> py vol.py -v -f "C:\Users\Shalom\Desktop\880522-10359-01.dmp" windows.info
Volatility 3 Framework 2.0.1
INFO volatility3.cli: Volatility plugins path: ['C:\\Users\\Shalom\\Downloads\\\\volatility3-2.0.1\\\\volatility3\\plugins', 'C:\\Users\\Shalom\\Downloads\\volatility3-2.0.1\\\\volatility3-2.0.1\\\\volatility3\\symbols']
INFO volatility3.cli: Volatility symbols path: ['C:\\Users\\Shalom\\Downloads\\\\volatility3-2.0.1\\\\volatility3\\symbols', 'C:\\Users\\Shalom\\Downloads\\volatility3-2.0.1\\\\volatility3-2.0.1\\\\volatility3\\symbols']
INFO volatility3.cli: The following plugins could not be loaded (use -vv to see why): volatility3.plugins.windows.cachedump, volatility3.plugins.windows.hashdump, volatility3.plugins.windows.lsadump
INFO volatility3.framework.automatic: Detected a windows category plugin
INFO volatility3.framework.automatic: Running automatic: ConstructionMagic
INFO volatility3.framework.automatic: Running automatic: LayerStacker
INFO volatility3.schemas: Dependency for validation unavailable: jsonschema
INFO volatility3.schemas: Dependency for validation unavailable: jsonschema
INFO volatility3.framework.automatic: Running automatic: WinMapPlayers
INFO volatility3.framework.automatic: Running automatic: KernelPOBScanner
INFO volatility3.framework.automatic: No suitable kernels found during pdbscan
INFO volatility3.framework.automatic: Running automatic: KernelModule

unsatisfied requirement.plugins.Info.kernel: Windows kernel
unable to validate the plugin requirements: ['plugins.Info.kernel']
```

## 11. Conclusion: Memory analysis has been successfully done

## 12. Reference:

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

<https://neoslab.com/2020/04/28/how-to-extract-data-from-windows-memory-dump-using-volatility-cUNHMLhCTmxtTGdENEhRek1NWTlOdz09>

<https://blog.cyberhacktcs.com/memory-forensics-on-windows-10-with-volatility/>

<https://github.com/volatilityfoundation/volatility3>

<https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765>

<https://www.youtube.com/watch?v=gHbejxlPbRQ>

<https://www.hackingarticles.in/multiple-ways-to-capture-memory-for-analysis/>

## Lab Assignment 2

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 2
- 4. Title of the Program/Experiment:** Wireshark & Autopsy
- 5. Date Program/Experiment Performed:** 31/08/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To analyze Windows & Unix file systems using Autopsy and analyze packets using Wireshark

### **8. Description:**

#### a. Overview

We have to analyze Linux file system using Autopsy tool.

#### b. System Requirement: (Software and Hardware)

- 64-bit AMD64/x86-64 or 32-bit x86 CPU architecture.
- At least 500 MB available RAM
- At least 500 MB of available disk space
- It requires a minimum resolution of  $1280 \times 1024$  or higher.
- A Windows, Linux, or Mac OS X machine
- Wireshark tool
- Autopsy tool

#### c. Configuration of the System used by you to perform the experiment/installation

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

#### d. Algorithm (Step by Step Approach)

No algorithms were used

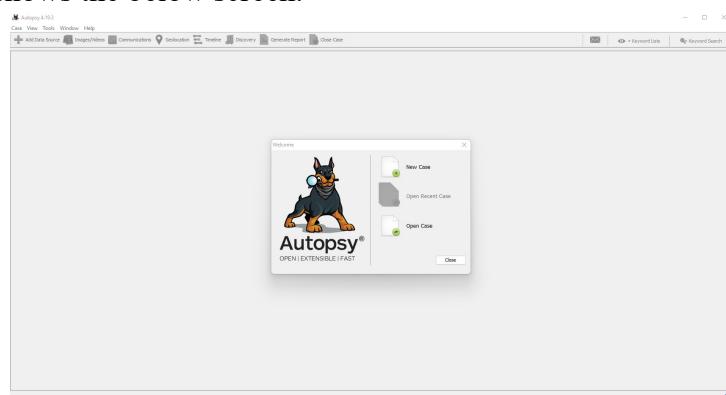
### **9. Implementation Details:**

#### a. In case of programming implementation: Please add source code

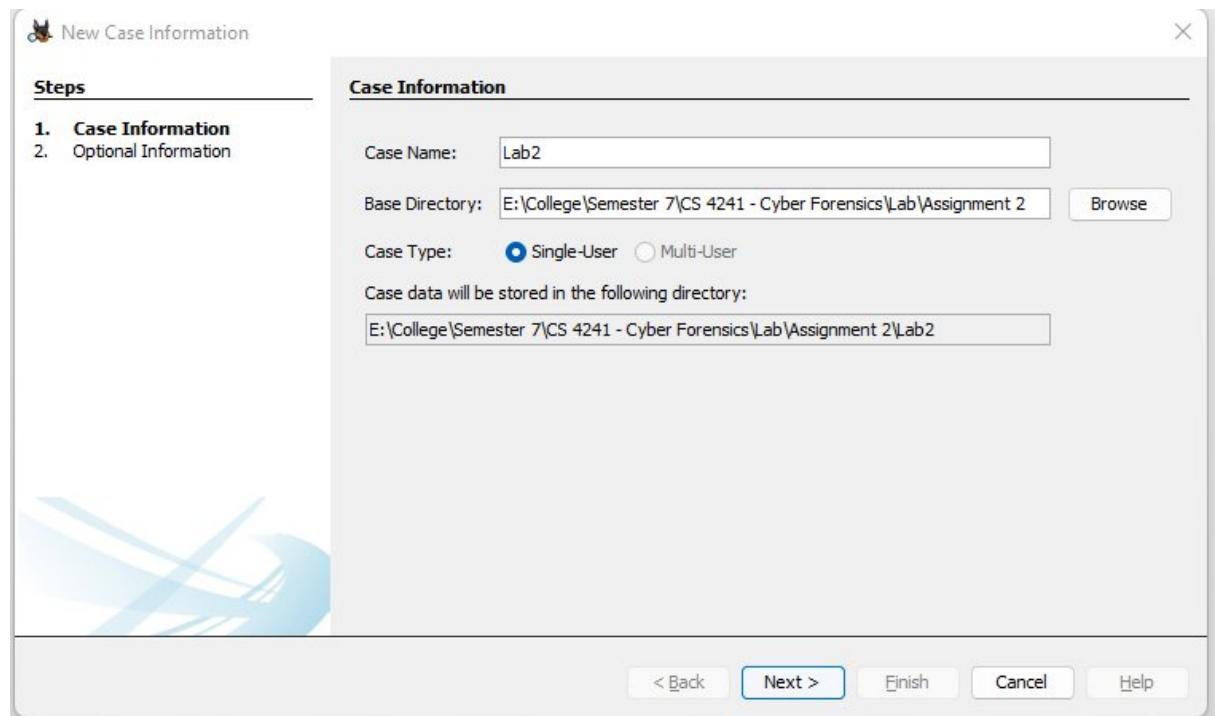
No programming was done.

#### b. In case of software installation: Please add screenshots. (Step by Step)

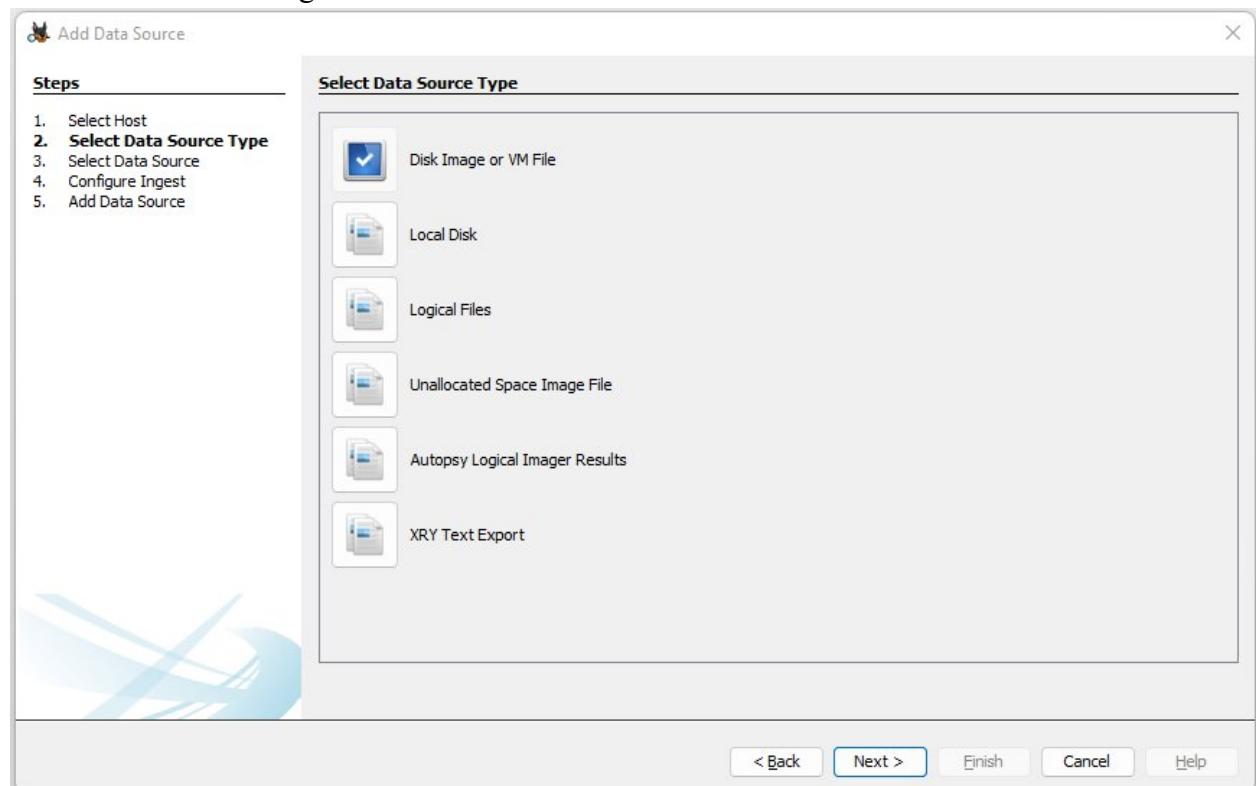
Autopsy tool was downloaded from <https://www.autopsy.com/download/>. Opening the application shows the below screen.

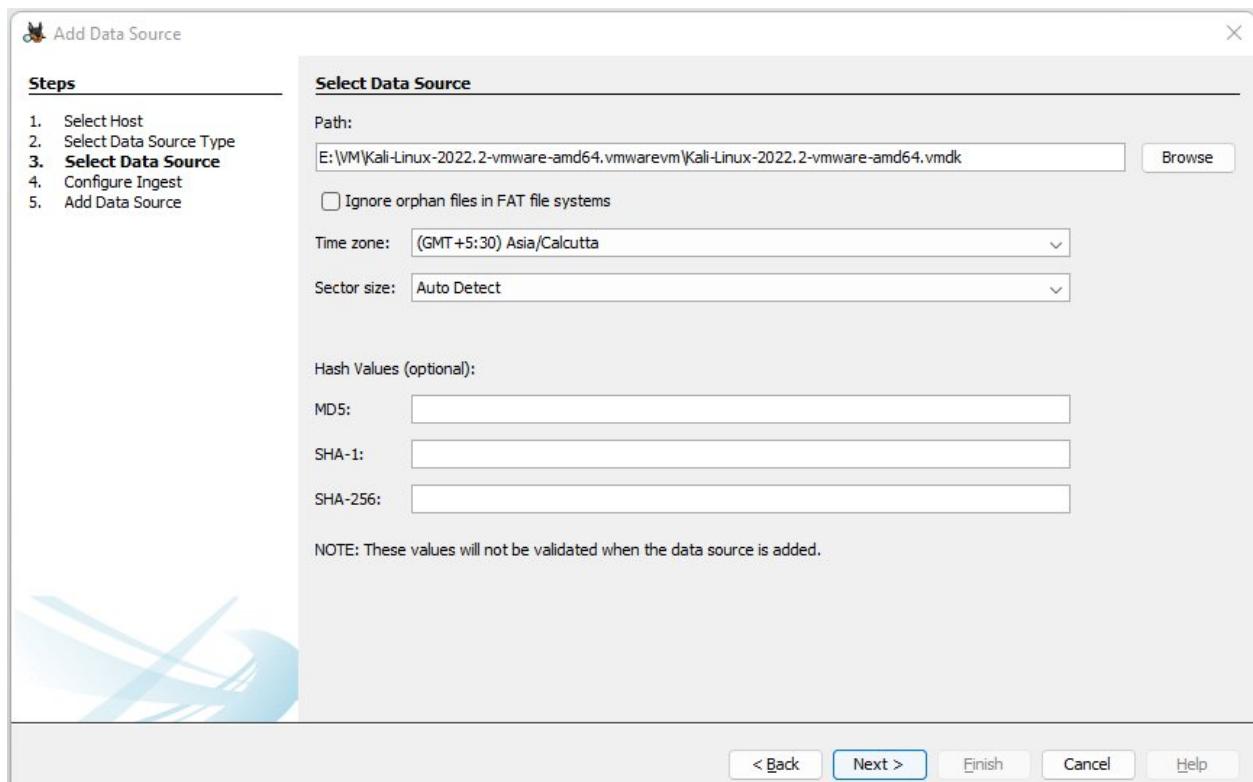


A new case is created and relevant details are entered

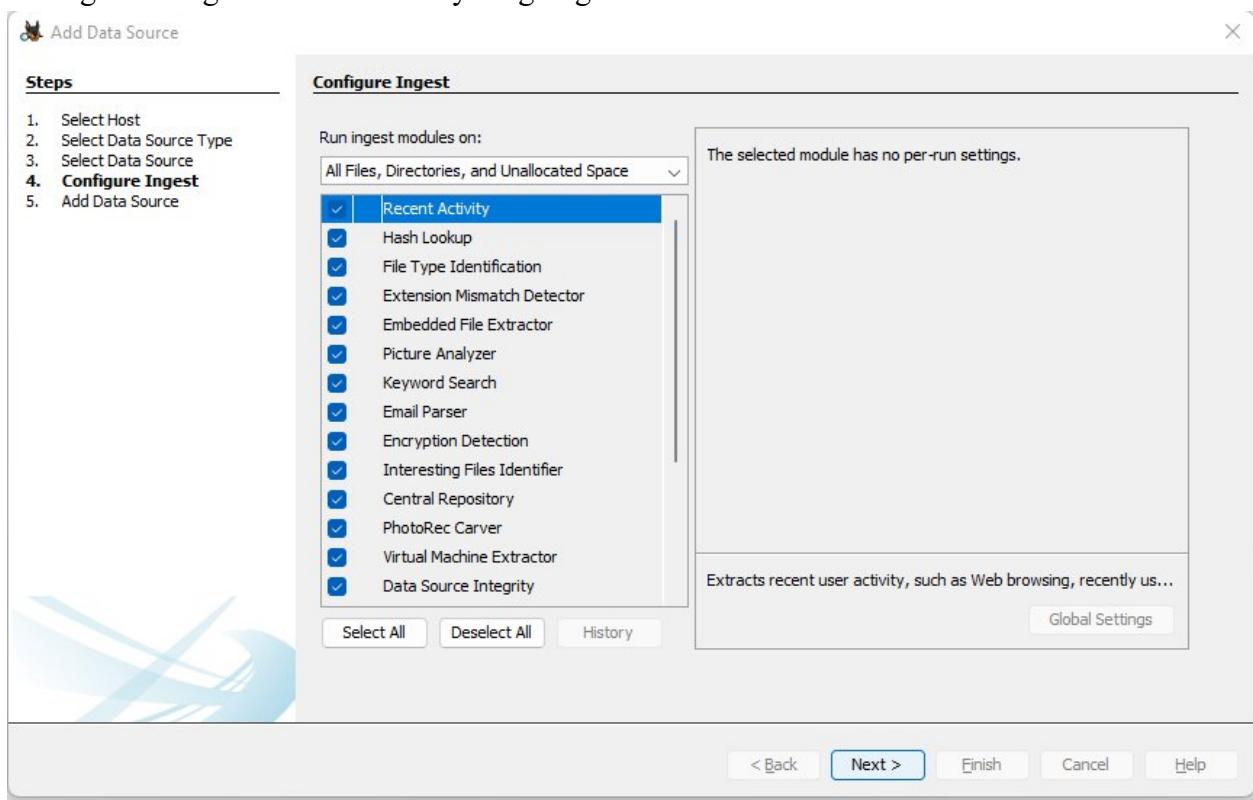


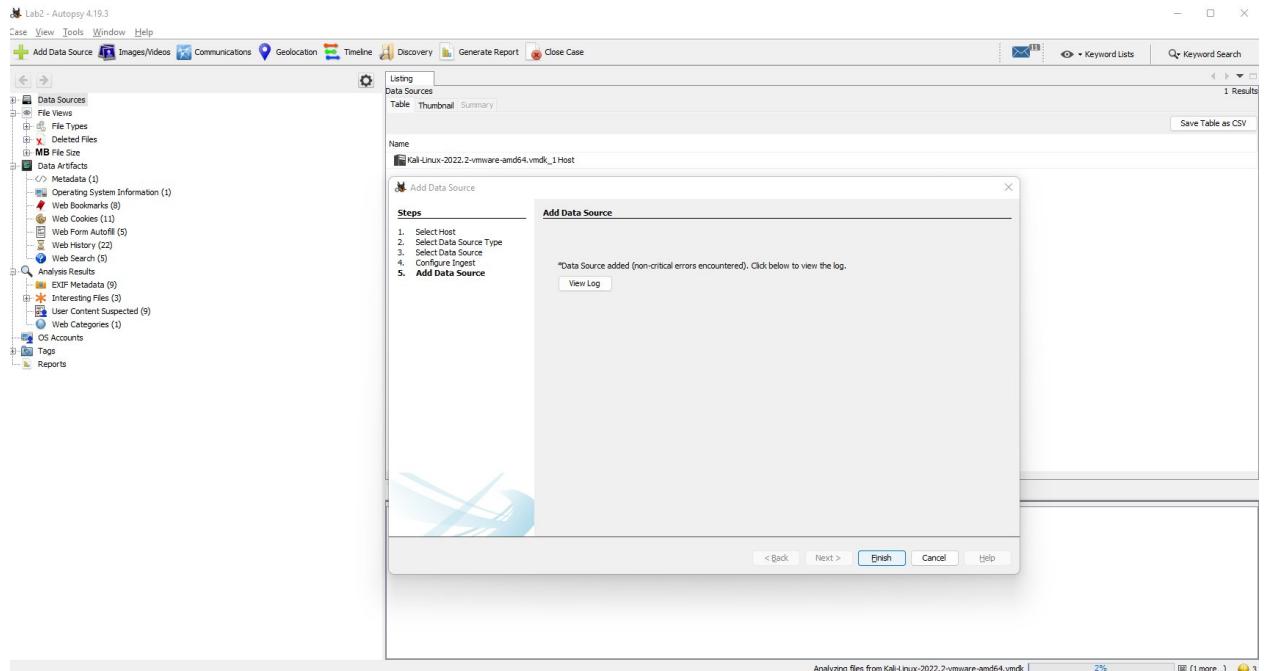
A Kali-Linux VM image will be chosen as a data source





Configure to ingest to include everything to get all information





Now we can see the dashboard and all the important information

## Bookmarks

Source Name	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source
places.sqlite	0			https://www.kali.org/docs/	Kali Docs	2022-06-24 17:18:12 IST	Firefox	kali.org	Kali-Linux-2022-2-vmware-amd64.vmdk
places.sqlite	0			https://forums.kali.org/	Kali Forums	2022-06-24 17:18:12 IST	Firefox	kali.org	Kali-Linux-2022-2-vmware-amd64.vmdk
places.sqlite	0			https://www.kali.org/kali-nethunter/	Kali NetHunter	2022-06-24 17:18:12 IST	Firefox	kali.org	Kali-Linux-2022-2-vmware-amd64.vmdk
places.sqlite	0			https://www.exploit-db.com/	Exploit-DB	2022-06-24 17:18:12 IST	Firefox	exploit-db.com	Kali-Linux-2022-2-vmware-amd64.vmdk
places.sqlite	0			https://www.exploit-db.com/google-hacking-database	Google Hacking DB	2022-06-24 17:18:12 IST	Firefox	exploit-db.com	Kali-Linux-2022-2-vmware-amd64.vmdk
places.sqlite	0			https://www.offensive-security.com/	OffSec	2022-06-24 17:18:12 IST	Firefox	offensive-security.com	Kali-Linux-2022-2-vmware-amd64.vmdk

## Cookies

Source Name	S	C	O	URL	Date Accessed	Name	Value	Program Name	Date Created	Domain
cookies.sqlite	1			youtube.com	2022-06-24 17:18:25 IST	GPS	1	Firefox	2022-06-24 17:18:25 IST	youtube
cookies.sqlite	1			youtube.com	2022-06-24 17:18:25 IST	VISITOR_INFO1_LIVE	CO_RuWqPKA	Firefox	2022-06-24 17:18:25 IST	youtube
cookies.sqlite	1			accounts.google.com	2022-06-24 17:18:25 IST	_JHost-GAPS	1:201w61y1n10WOGd3h3Xt523GoUaw:OlpCHp9D0oep5r	Firefox	2022-06-24 17:18:25 IST	google.com
cookies.sqlite	1			youtube.com	2022-06-24 17:18:25 IST	PREF	tz=America.New_York	Firefox	2022-06-24 17:18:26 IST	youtube
cookies.sqlite	1			.google.com	2022-06-24 17:18:25 IST	AaInG0gBsaUY0c11MFq3lWhOHnV2mblVjU_3pAeq...	Firefox	2022-06-24 17:18:26 IST	google.com	

## Deleted Files

Screenshot of the Autopsy Forensic Browser showing deleted files analysis.

**Deleted Files:**

- File System (15544)
- All (15544)

**Analysis Results:**

- EXIF Metadata (10)
- Extension Mismatch Detected (30)
- Interesting Files (19)
- Keyword Hits (10498)
- User Content Suspected (10)
- Web Categories (1)

**Hex View:**

```
# Copyright (c) 2017-2019, PyInstaller Development Team.
# Distributed under the terms of the GNU General Public License with exception
# for distributing bootloader.
#
# The full license is in the file COPYING.txt, distributed with this software.

from PyInstaller.utils.hooks import copy_metadata
datas = copy_metadata('google-cloud-storage')
```

**Metadata:**

## Web History

Screenshot of the Autopsy Forensic Browser showing web history analysis.

**Deleted Files:**

- File System (15544)
- All (15544)

**Analysis Results:**

- EXIF Metadata (10)
- Extension Mismatch Detected (30)
- Interesting Files (19)
- Keyword Hits (10498)
- User Content Suspected (10)
- Web Categories (1)

**Visit Details:**

Title	URL	Date Accessed	Referrer URL	Title	Program Name
The birth of the Web   CERN	http://info.cern.ch/	2022-08-30 17:09:23 IST		http://info.cern.ch/	Firefox
The World Wide Web project	http://info.cern.ch/hyperText/WWW/TheProject.html	2022-08-30 17:12:02 IST	http://info.cern.ch/	The World Wide Web project	Firefox
The World Wide Web project	http://info.cern.ch/hyperText/WWW/TheProject.html	2022-08-30 17:18:44 IST	http://info.cern.ch/	The World Wide Web project	Firefox
The birth of the Web   CERN	https://home.web.cern.ch/science/computing/birth-web	2022-08-30 17:18:51 IST	https://home.web.cern.ch/topics/birth-web	The birth of the Web   CERN	Firefox

## Images

Screenshot of the Autopsy Forensic Browser showing images analysis.

**Deleted Files:**

- File System (15544)
- All (15544)

**Analysis Results:**

- EXIF Metadata (10)
- Extension Mismatch Detected (30)
- Interesting Files (19)
- Keyword Hits (10498)
- User Content Suspected (10)
- Web Categories (1)

**Image Preview:**

## Data Files

The screenshot shows a digital forensics tool's interface. On the left is a tree view of the analyzed system:

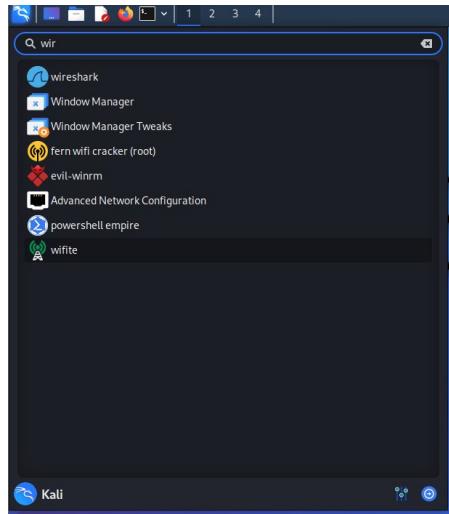
- Data Sources
  - File Views
    - By Extension
      - Images (17280)
      - Videos (35)
      - Aux (66)
      - Archives (13712)
      - Databases (49)
      - Documents
      - Executable
      - By MIME Type
    - Deleted Files
      - File System (15544)
      - All (15544)
  - MB File Size
  - Data Artifacts
    - Communication Accounts (20)
    - E-Mail Messages (22)
      - Default ([Default])
        - Default (22)
    - Metadata (28)
    - Operating System Information (1)
    - Web Bookmarks (8)
    - Web Cookies (11)
    - Web Form Autofill (5)
    - Web History (22)
    - Web Search (5)

Listing Metadata								Save Table as CSV			
Table		Thumbnail		Summary							
Page: 1 of 1		Pages: < > Go to Page:		S	C	O	Version	Date Modified	Date Created	Data Source	Owner
✓ Microsoft_Office_Excel_Worksheet6.xlsx								2013-10-06 20:47:16 IST	2013-10-06 20:47:14 IST	Kali-Linux-2022.2-vmware-andf4.vmdk	fr3akWin7x64
✓ Microsoft_Office_Excel_Worksheet1.xlsx								2013-10-06 20:47:46 IST	2013-10-06 20:47:45 IST	Kali-Linux-2022.2-vmware-andf4.vmdk	fr3akWin7x64
✓ User_Manual.pdf							1.3	2014-05-01 01:11:37 IST	2014-05-01 01:11:37 IST	Kali-Linux-2022.2-vmware-andf4.vmdk	Dave
✓ form.pdf							1.3	2009-08-30 00:20:17 IST	2009-08-30 00:20:17 IST	Kali-Linux-2022.2-vmware-andf4.vmdk	Department of Justice (Executive Office of In
✓ fleasave.pdf							1.4	2016-06-01 16:35:07 IST	2016-06-01 16:35:07 IST	Kali-Linux-2022.2-vmware-andf4.vmdk	

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences	Metadata
Result: 1 of 1	Result	< >								
Type	Value									Source(s)
Version	1.3									org.sleuthkit.autopsy.keyword
Date Modified	2009-08-30 00:20:17 IST									org.sleuthkit.autopsy.keyword
Date Created	2009-08-30 00:20:17 IST									org.sleuthkit.autopsy.keyword
Owner	Department of Justice (Executive Office of Immigration Review)									org.sleuthkit.autopsy.keyword
Source File Path	/img_Kali-Linux-2022.2-vmware-andf4.vmdk/vol_vd2/usr/share/kali/src/core/msf_attacks/form.pdf									org.sleuthkit.autopsy.keyword
Artifact ID	4223372036854765128									

Now, moving on to Wireshark



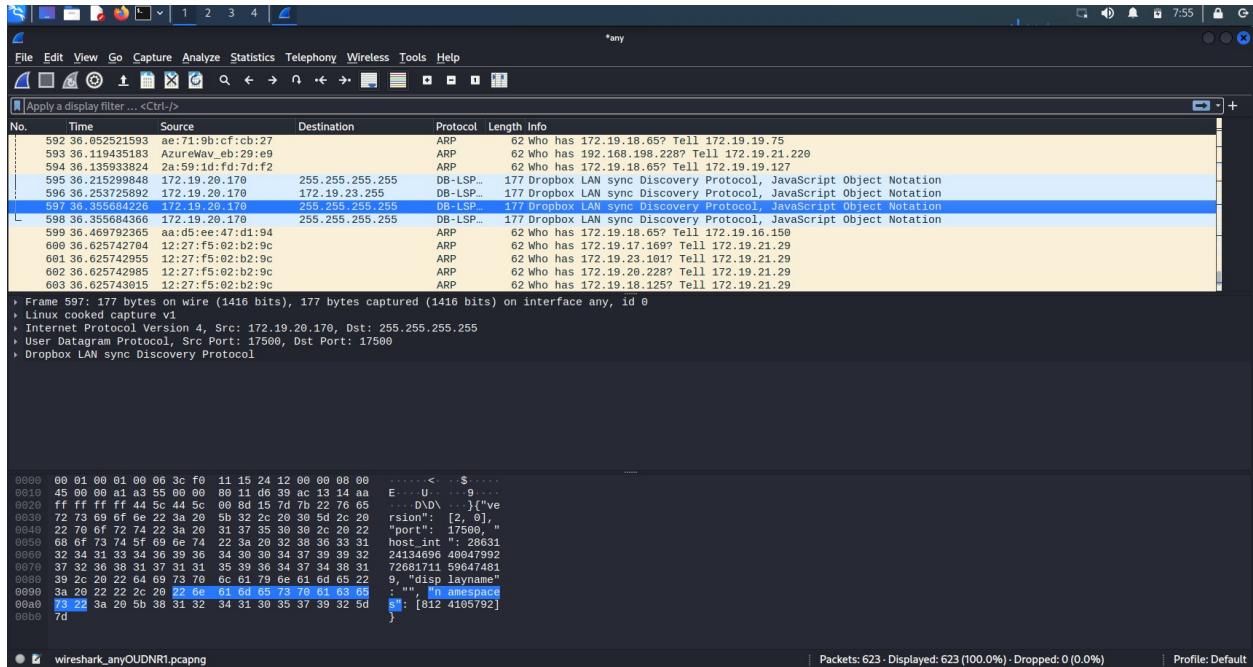
Opening wireshark greets us with this dashboard

The screenshot shows the Wireshark Network Analyzer dashboard. At the top, it says "Welcome to Wireshark". Below that is the "Capture" section with a "using this filter:" input field containing "Enter a capture filter ...". A dropdown menu "All interfaces shown" is open. The interface list shows:

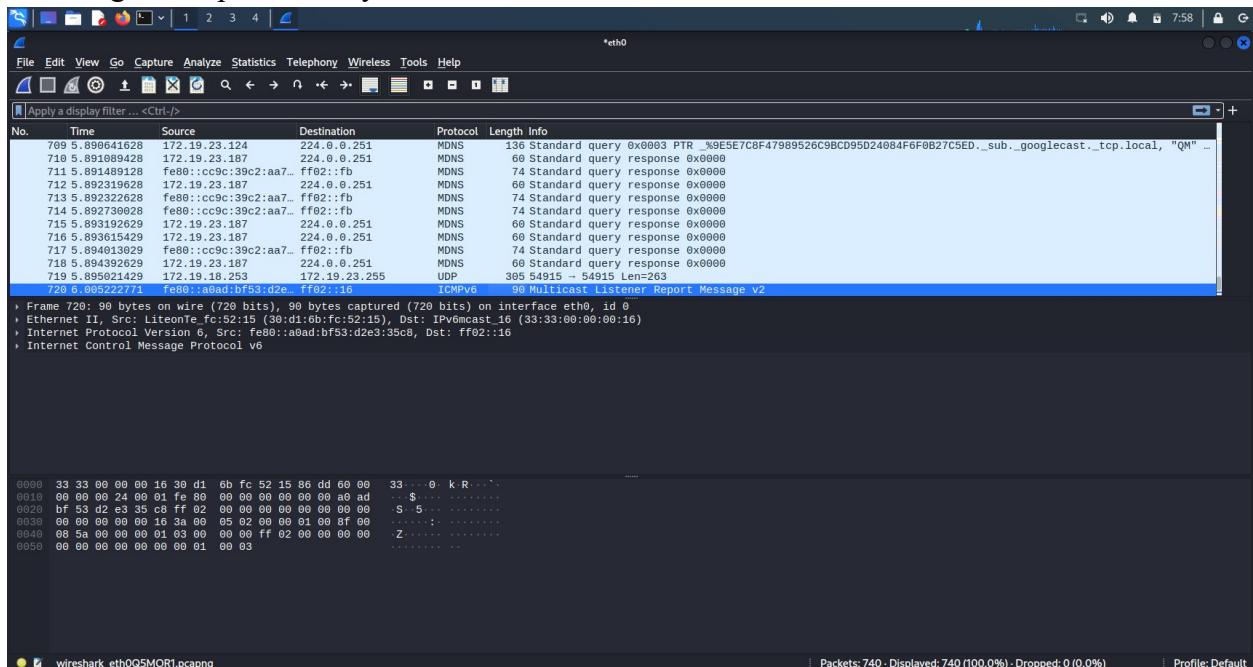
- eth0
- any
- Loopback: lo
- bluetooth-monitor
- nfqueue
- nfqueue
- dbus-system
- dbus-session
- (Cisco remote capture: ciscodump
- (DisplayPort AUX channel monitor capture: dpauxmon
- (Random packet generator: randpkt
- (systemd Journal Export: sdjournal
- (SSH remote capture: sshdump
- (UDP Listener remote capture: udpcap

At the bottom of the dashboard, there is a "Learn" section with links to "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". It also states "You are running Wireshark 3.6.3 (Git v3.6.3 packaged as 3.6.3-1)". The status bar at the bottom indicates "Ready to load or capture", "No Packets", and "Profile: Default".

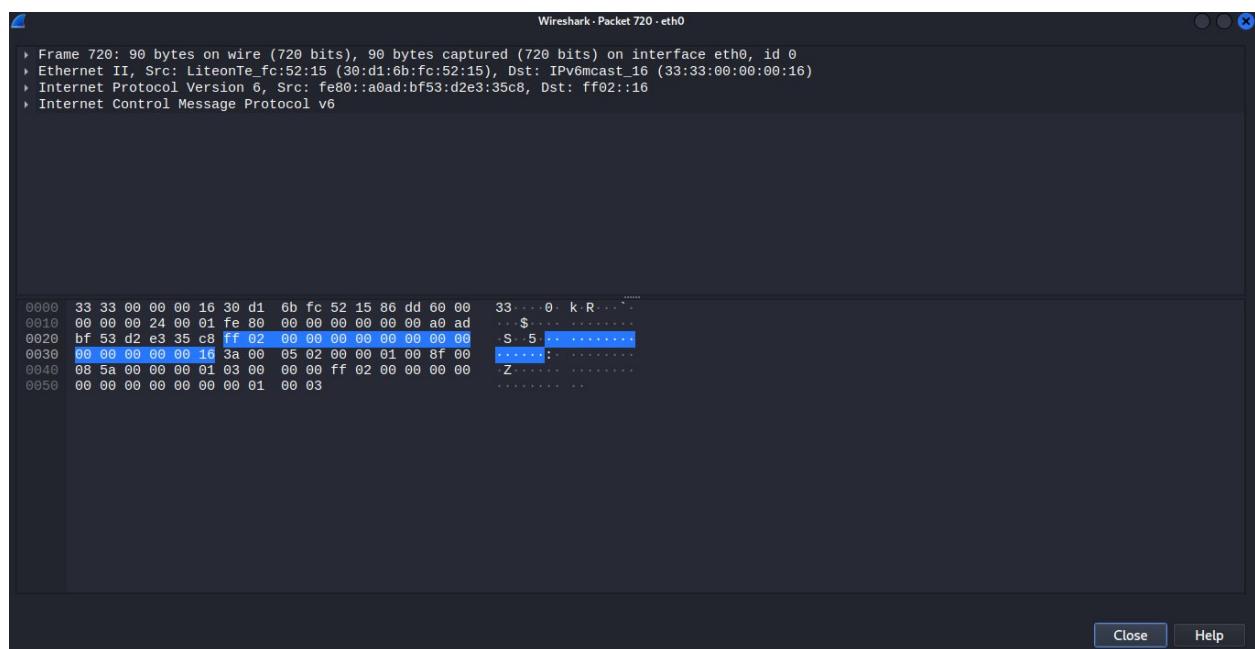
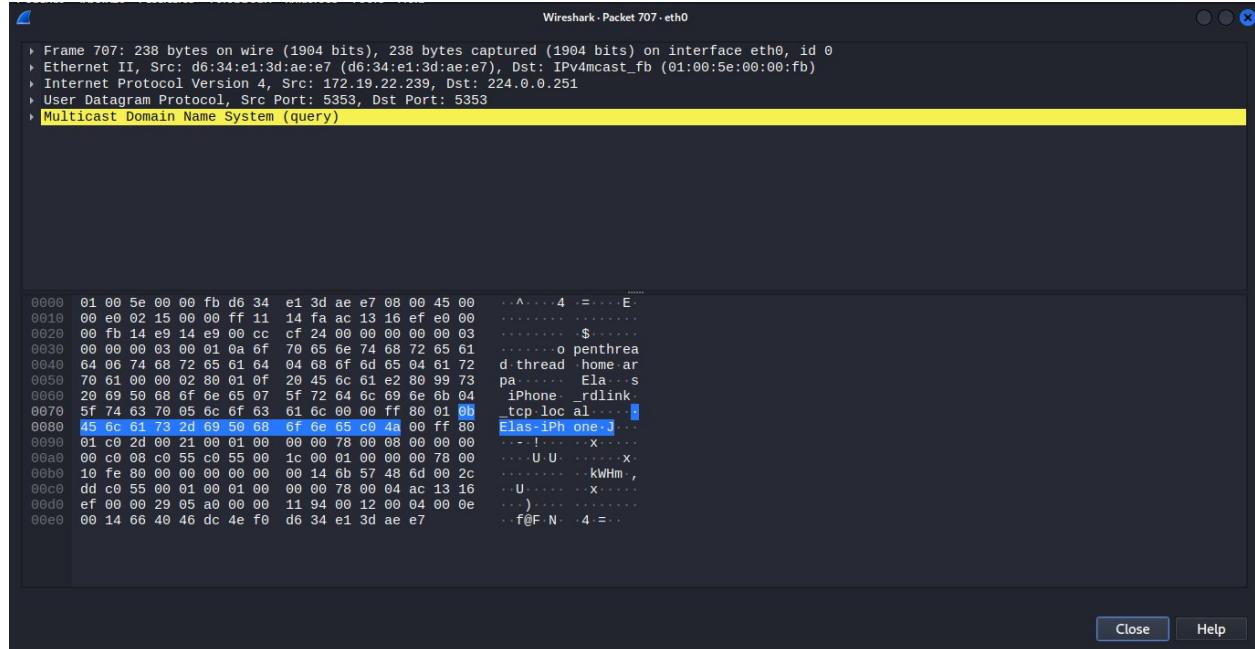
Starting capture of data packets lets us see the data packets travelling and their details



Selecting a data packet lets you know its contents



Double clicking on it gives a more detailed view about it



## 10. Error Description:

No errors were faced

**11. Conclusion:** Disk forensics has been successfully completed and analysis of data packets has been done using Wireshark

## 12. Reference:

<https://www.autopsy.com/download/>

<https://www.wireshark.org/>

## Lab Assignment 3

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 3
- 4. Title of the Program/Experiment:** EXIF Tool
- 5. Date Program/Experiment Performed:** 21/09/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To read metadata of files using EXIFTool

**8. Description:**

a. **Overview**

We have to read, write, and manipulate image, audio, video, and PDF metadata.

b. **System Requirement: (Software and Hardware)**

- Perl 5.004 or later
- At least 500 MB available RAM
- At least 500 MB of available disk space
- A Windows, Linux, or Mac OS X machine
- EXIF tool

c. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

d. **Algorithm (Step by Step Approach)**

No algorithms were used

**9. Implementation Details:**

a. **In case of programming implementation: Please add source code**

No programming was done.

b. **In case of software installation: Please add screenshots. (Step by Step)**

Download EXIFTool from <https://exiftool.org/index.html#running>. After successful download, Run the tool using terminal after extracting and removing (-k) from the .exe tool

```
PS C:\Users\Shalom> cd "C:\Users\Shalom\Downloads\exiftool-12.45"
PS C:\Users\Shalom\Downloads\exiftool-12.45> ./exiftool -v C:\Users\Shalom\Desktop\contract.sol
ExifToolVersion = 12.45
FileName = contract.sol
Directory = C:/Users/Shalom/Desktop
FileSize = 1515
FileModifyDate = 1662629628
FileAccessDate = 1663758383.69242
FileCreateDate = 1662649477.22618
FilePermissions = 33206
FileType = TXT
FileTypeExtension = TXT
MIMEType = text/plain
MIMEEncoding = us-ascii
Newlines = ..
LineCount = 51
WordCount = 164
```

Different commands can be used to get more and different metadata about various files

```
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool C:\Users\Shalom\Desktop\contract.sol
ExifTool Version Number      : 12.45
File Name                   : contract.sol
Directory                   : C:/Users/Shalom/Desktop
File Size                    : 1515 bytes
File Modification Date/Time : 2022:09:08 15:03:48+05:30
File Access Date/Time       : 2022:09:21 16:41:02+05:30
File Creation Date/Time    : 2022:09:08 20:34:37+05:30
File Permissions            : -rw-rw-rw-
File Type                   : TXT
File Type Extension         : txt
MIME Type                   : text/plain
MIME Encoding               : us-ascii
Newlines                     : Windows CRLF
Line Count                  : 51
Word Count                  : 164
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool -h C:\Users\Shalom\Desktop\contract.sol
<!-- C:/Users/Shalom/Desktop/contract.sol -->
<table>
<tr><td>ExifTool Version Number</td><td>12.45</td></tr>
<tr><td>File Name</td><td>contract.sol</td></tr>
<tr><td>Directory</td><td>C:/Users/Shalom/Desktop</td></tr>
<tr><td>File Size</td><td>1515 bytes</td></tr>
<tr><td>File Modification Date/Time</td><td>2022:09:08 15:03:48+05:30</td></tr>
<tr><td>File Access Date/Time</td><td>2022:09:21 16:41:07+05:30</td></tr>
<tr><td>File Creation Date/Time</td><td>2022:09:08 20:34:37+05:30</td></tr>
<tr><td>File Permissions</td><td>-rw-rw-rw-</td></tr>
<tr><td>File Type</td><td>TXT</td></tr>
<tr><td>File Type Extension</td><td>txt</td></tr>
<tr><td>MIME Type</td><td>text/plain</td></tr>
<tr><td>MIME Encoding</td><td>us-ascii</td></tr>
<tr><td>Newlines</td><td>Windows CRLF</td></tr>
<tr><td>Line Count</td><td>51</td></tr>
<tr><td>Word Count</td><td>164</td></tr>
</table>
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool -h C:\Users\Shalom\Desktop\th-259025762.jpg
<!-- C:/Users/Shalom/Desktop/th-259025762.jpg -->
<table>
<tr><td>ExifTool Version Number</td><td>12.45</td></tr>
<tr><td>File Name</td><td>th-259025762.jpg</td></tr>
<tr><td>Directory</td><td>C:/Users/Shalom/Desktop</td></tr>
<tr><td>File Size</td><td>96 kB</td></tr>
<tr><td>Zone Identifier</td><td>Exists</td></tr>
<tr><td>File Modification Date/Time</td><td>2022:08:21 18:32:14+05:30</td></tr>
<tr><td>File Access Date/Time</td><td>2022:09:21 17:09:57+05:30</td></tr>
<tr><td>File Creation Date/Time</td><td>2022:08:21 18:32:14+05:30</td></tr>
<tr><td>File Permissions</td><td>-rw-rw-rw-</td></tr>
<tr><td>File Type</td><td>JPEG</td></tr>
<tr><td>File Type Extension</td><td>jpg</td></tr>
<tr><td>MIME Type</td><td>image/jpeg</td></tr>
<tr><td>JFIF Version</td><td>1.01</td></tr>
<tr><td>Resolution Unit</td><td>inches</td></tr>
<tr><td>X Resolution</td><td>0</td></tr>
<tr><td>Y Resolution</td><td>0</td></tr>
<tr><td>Exif Byte Order</td><td>Big-endian (Motorola, MM)</td></tr>
<tr><td>Image Width</td><td>474</td></tr>
<tr><td>Image Height</td><td>1030</td></tr>
<tr><td>Encoding Process</td><td>Baseline DCT, Huffman coding</td></tr>
<tr><td>Bits Per Sample</td><td>8</td></tr>
<tr><td>Color Components</td><td>3</td></tr>
<tr><td>Y Cb Cr Sub Sampling</td><td>YCbCr4:2:0 (2 2)</td></tr>
<tr><td>Image Size</td><td>474x1030</td></tr>
<tr><td>Megapixels</td><td>0.488</td></tr>
</table>
```

## 10. Error Description:

Had to use .\exiftool instead of exiftool

```
PS C:\Users\Shalom\Downloads\exiftool-12.45> exiftool -h
exiftool : The term 'exiftool' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ exiftool -h
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (exiftool:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

Suggestion [3,General]: The command exiftool was not found, but does exist in the current location. Windows PowerShell d
oes not load commands from the current location by default. If you trust this command, instead type: ".\exiftool". See "get-help about_Command_Precedence" for more details.
PS C:\Users\Shalom\Downloads\exiftool-12.45>
```

**11. Conclusion:** Metadata about various files has been successfully observed using EXIFTool

**12. Reference:**

<https://www.exiftool.org/dummies.html>

<https://twistandclick.com/2022/02/03/using-exiftool-a-beginners-guide/>

## Lab Assignment 4

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 4
- 4. Title of the Program/Experiment:** BruteShark & LiveForensicator
- 5. Date Program/Experiment Performed:** 28/09/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To analyze network traffic using BruteShark & gather system information using LiveForensicator

### **8. Description:**

#### **a. Overview**

We have to perform network traffic analysis to identify weaknesses using BruteShark. We also need to gather different system information for further review for anomalous behaviour or unexpected data entry using Live Forensicator.

#### **b. System Requirement: (Software and Hardware)**

- Npcap driver/libpcap driver
- At least 500 MB available RAM
- At least 500 MB of available disk space
- A Windows, Linux, or Mac OS X machine
- BruteSharkCLI tool
- Live Forensicator tool

#### **c. Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

#### **d. Algorithm (Step by Step Approach)**

No algorithms were used

### **9. Implementation Details:**

#### **a. In case of programming implementation: Please add source code**

No programming was done.

#### **b. In case of software installation: Please add screenshots. (Step by Step)**

Install Bruteshark in a Linux Machine

```
kali@kali: ~
File Actions Edit View Help
95% [3 Contents-amd64 store 0 B] 1,636 kB/s 0s^
Fetched 63.7 MB in 43s (1,498 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1383 packages can be upgraded. Run 'apt list --upgradable' to see them.

[(kali㉿kali)-[~]
$ sudo apt install bruteshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  bruteshark
0 upgraded, 1 newly installed, 0 to remove and 1383 not upgraded.
Need to get 31.1 MB of archives.
After this operation, 97.8 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/contrib amd64 bruteshark amd64 1
.2.5-0kali7 [31.1 MB]
Fetched 31.1 MB in 5s (6,108 kB/s)
Selecting previously unselected package bruteshark.
(Reading database ... 338510 files and directories currently installed.)
Preparing to unpack .../bruteshark_1.2.5-0kali7_amd64.deb ...
Unpacking bruteshark (1.2.5-0kali7) ...
Setting up bruteshark (1.2.5-0kali7) ...
Processing triggers for kali-menu (2022.3.1) ...
```

Use the help function to see how to use it

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ brutesharkcli --help
BruteSharkCli 1.0.0.0
Copyright © 2018

-d, --input-dir      The input directory containing the files to be
                     processed.

-i, --input          The files to be processed separated by comma.

-m, --modules        The modules to be separated by comma: Credentials,
                     FileExtracting, NetworkMap, DNS, Voip.

-o, --output         Output directory for the results files.

-p, --promiscuous   Configures whether to start live capture with
                     promiscuous mode (sometimes needs super user
                     privileges to do so), use along with -l for live
                     capture.

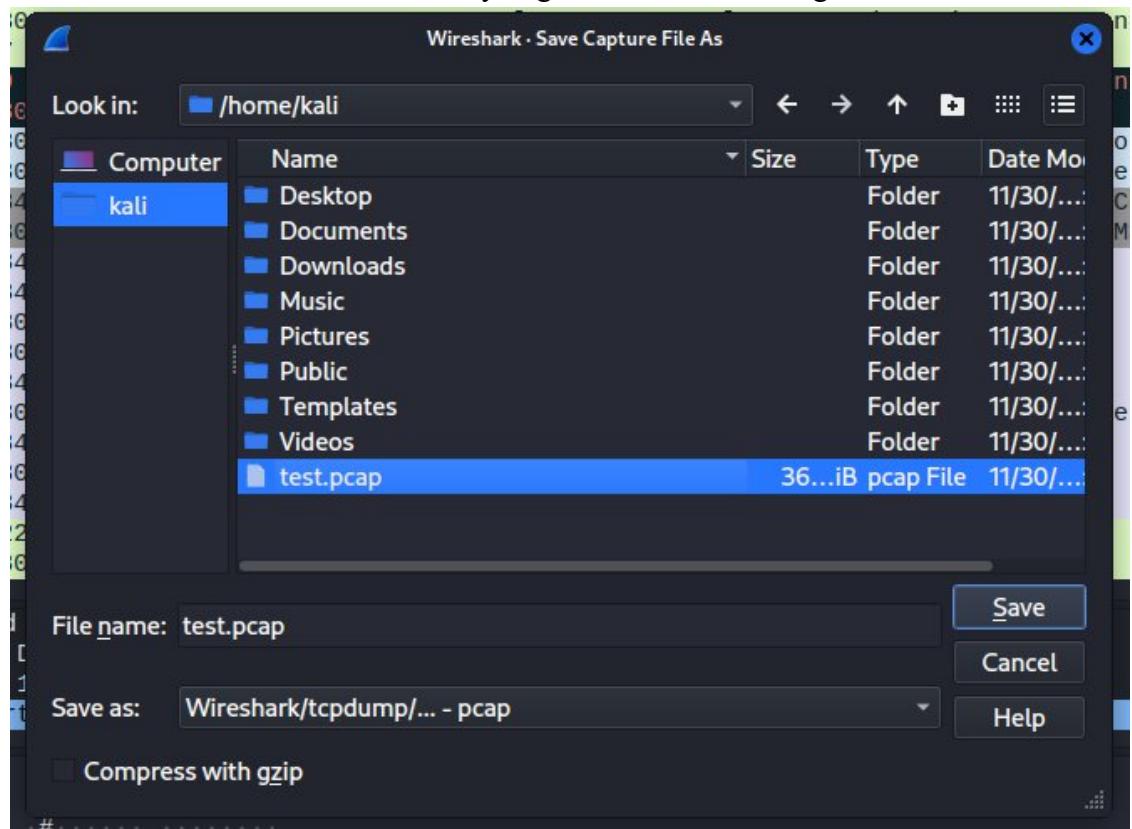
-l, --live-capture  Capture and process packets live from a network
                     interface.

-f, --filter         Set a capture BPF filter to the live traffic
                     processing.

--help               Display this help screen.

--version            Display version information.
```

### Get PCAP file after analyzing network traffic using Wireshark



Run various commands to get information about the newly generated PCAP file

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ brutesharkcli -m DNS -i test.pcap
[+] Start analyzing 1 files
[+] Start processing file : test.pcap
Found: DNS Mapping: firefox-settings-attachments.cdn.mozilla.net → fennec
talog-cdn.prod.mozaws.net
Found: DNS Mapping: firefox-settings-attachments.cdn.mozilla.net → 34.160
.51
Found: DNS Mapping: tracking-protection.cdn.mozilla.net → tracking-protec
n.prod.mozaws.net
Found: DNS Mapping: tracking-protection.cdn.mozilla.net → 34.120.158.37
Found: DNS Mapping: play.google.com → 142.250.192.78
Found: DNS Mapping: play.google.com → 2404:6800:4009:829::200e
Found: DNS Mapping: apis.google.com → plus.l.google.com
Found: DNS Mapping: apis.google.com → 142.250.183.110
Found: DNS Mapping: apis.google.com → 2404:6800:4009:823::200e
Found: DNS Mapping: adservice.google.com → 172.217.167.162
Found: DNS Mapping: adservice.google.com → 2404:6800:4009:830::2002
Found: DNS Mapping: adservice.google.co.in → pagead46.l.doubleclick.net
Found: DNS Mapping: adservice.google.co.in → 142.250.192.34
Found: DNS Mapping: adservice.google.co.in → 2404:6800:4009:831::2002
[+] Finished processing file : test.pcap
[+] BruteShark finished processing
```

```
(kali㉿kali)-[~]
└─$ sudo brutesharkcli -m voip -l eth0
[+] Started analyzing packets from eth0 device - Press Ctrl + C to stop
[  ]
```

```
(kali㉿kali)-[~]
└─$ sudo brutesharkcli -m DNS -l eth0 -p
[+] Started analyzing packets from eth0 device (Promiscuous mode) - Press Ctrl + C to stop
Found: DNS Mapping: push.services.mozilla.com → autopush.prod.mozaws.net
Found: DNS Mapping: push.services.mozilla.com → 34.214.236.46
Found: DNS Mapping: push.services.mozilla.com → 52.13.173.34
Found: DNS Mapping: push.services.mozilla.com → 54.148.84.125
Found: DNS Mapping: example.org → 93.184.216.34
Found: DNS Mapping: ipv4only.arpa → 192.0.0.171
Found: DNS Mapping: ipv4only.arpa → 192.0.0.170
Found: DNS Mapping: example.org → 2606:2800:220:1:248:1893:25c8:1946
Found: DNS Mapping: detectportal.firefox.com → detectportal.prod.mozaws.net
Found: DNS Mapping: detectportal.firefox.com → prod.detectportal.prod.cloudops.mozgcp.net
Found: DNS Mapping: detectportal.firefox.com → 34.107.221.82
Found: DNS Mapping: detectportal.firefox.com → 2600:1901:0:38d7::1
Found: DNS Mapping: push.services.mozilla.com → 35.160.184.41
Found: DNS Mapping: push.services.mozilla.com → 54.148.69.31
Found: DNS Mapping: push.services.mozilla.com → 34.218.168.248
Found: DNS Mapping: push.services.mozilla.com → 54.186.169.128
[  ]
```

Clone the github repository of Live Forensicator and execute the application. The below screen will be shown.



v3.2.1

```
[!] Live Forensicator
[!] Examines the host for suspicious activities and grabs required data for further forensics.
[!] By Ebuka John Onyejegbu.
[!] https://github.com/Johnng007/Live-Forensicator
[!] https://john.ng

Enter Investigator Name: Shalom
Enter Case Reference: 123456
Enter Investigation Title: Sample
Enter examination location: NU
Enter description of device e.g. "Asus Laptop": Laptop

[*] Gathering Network & Network Settings
[!] Done
[*] Gathering User & Account Information
[!] Done
[*] Gathering Installed Programs
[!] Done
[*] Gathering System Information
[!] Done
[*] Gathering Processes and Tasks
[!] Done
[*] Checking Registry for persistance
[!] Done
[*] Running Peripheral Checks...
[*] Entering Event Log Analysis Mode
[*] Checking Enumerated Users
[!] Done
[*] Fetching RDP Logons
[!] Done
[*] Fetching Created Users
[!] Done
[*] Checking for password resets
[!] Done
```

After all data is collected, the information collected is showcased in the below format

The screenshot shows the 'Live Forensicator' interface with the following details:

- Case reference:** 123456
- Examiner Name:** Shalom
- Exhibit reference:** Sample
- Device:** Laptop
- Examination Location:** NU
- Start Time and Date:** 2022-09-28 17:31:34
- End Time and Date:** 2022-09-28 17:34:19
- Browsing History:** View Browsing History
- Network Trace:** View PCAP FILES

PROCESSES   SCHEDULED TASK   REGISTRY											
▼ Processes											
Handles	StartTime	PM	VM	SI	Id	ProcessName	Path	Product	FileVersion		
173	28-09-2022 17:17:38	2138112	4408770560	3	13500	ACCMonitor	C:\Windows\System32\ASUSACCI\ACCMonitor.exe	Armoury Crate Control Interface Monitor	1.0.0.0		
418	28-09-2022 10:08:39	25677824	298315776	3	17180	AcPowerNotification	C:\Program Files (x86)\ASUS\ArmouryDevice\dl\AcPowerNotification\AcPowerNotification.exe	AcPowerNotification	1.0.5.12		
209	28-09-2022 11:18:26	2772992	88027136	3	13792	adb	C:\Users\Shalom\AppData\Local\Android\sdk\platform-tools\adb.exe				
93	26-09-2022 15:43:03	1019904	2203375808512	0	7016	AggregatorHost	C:\Windows\System32\AggregatorHost.exe				
299	28-09-2022 10:52:48	3530752	105652224	3	1896	Amazon Music Helper	C:\Program Files\WindowsApps\AmazonMobileLLC.AmazonMusic_9.2.1.0_x86_kc6t79cpj4tp0\Amazon Music Helper.exe	Amazon Music Helper	9.2.1.2362		
145	26-09-2022 15:43:00	2449408	4389457920	0	2760	amdfendrs	C:\Windows\System32\amdfendrs.exe	AMD Crash Defender Service	21.30.0.16		
611	28-09-2022 10:09:45	35774464	2203644669952	3	17092	ApplicationFrameHost	C:\Windows\System32\ApplicationFrameHost.exe	Microsoft Windows® Operating System	10.0.2000.1 (WinBuild.160101.0800)		
194	28-09-2022 10:08:57	2494464	4420640768	3	17104	ArmouryCrate.DenoiseAI	C:\Program Files\ASUS\ARMOURY CRATE Service\DenoiseAIPlugin\ArmouryCrate.DenoiseAI.exe	ARMOURY CRATE DenoiseAI	1.0.0.1		
1604	26-09-2022 15:43:03	115912704	5140914176	0	4912	ArmouryCrate.Service	C:\Program Files\ASUS\ARMOURY CRATE Service\ArmouryCrate.Service.exe	ARMOURY CRATE Service	5.2.5.0		
11892	28-09-2022 10:08:49	61775872	5163331584	3	11676	ArmouryCrate.UserSessionHelper	C:\Program Files\ASUS\ARMOURY CRATE Service\ArmouryCrate.UserSessionHelper.exe	ARMOURY CRATE Service	5.2.5.0		
322	26-09-2022 15:43:02	2596864	4385001472	0	4884	ArmouryCrateControlInterface	C:\Windows\System32\ASUSACCI\ArmouryCrateControlInterface.exe	Armoury Crate Control Interface	1.0.0.20		
276	28-09-2022 10:08:39	4595712	4449230848	3	24580	ArmourySocketServer	C:\Program Files (x86)\ASUS\ArmouryDevice\dl\ArmourySocketServer\ArmourySocketServer.exe	ArmourySocketServer	0.0.11.25		
288	28-09-2022 10:09:04	14856192	239124480	3	9104	ArmourySwAgent	C:\Program Files (x86)\ASUS\ArmouryDevice\dl\SwAgent\ArmourySwAgent.exe	ArmourySwAgent	2.0.0.17		
223	28-09-2022 10:08:39	1622016	4423852032	3	23732	AsHotplugCtrl	C:\Program Files\ASUS\ASUS Hotplug Controller\AsHotplugCtrl.exe	ASUS Hotplug Controller	2.0.0.0		
460	28-09-2022 10:08:56	28180480	322383872	3	5044	asus_framework	C:\Program Files (x86)\ASUS\ArmouryDevice\asus_framework.exe	ASUS NodeJS Web Framework	3.1.1.2		
277	28-09-2022 10:08:39	27918336	149217280	3	16820	asus_framework	C:\Program Files (x86)\ASUS\ArmouryDevice\asus_framework.exe	ASUS NodeJS Web Framework	3.1.1.2		
319	26-09-2022 15:43:02	5730304	4457390080	0	4996	AsusAppService	C:\Windows\System32\DriverStore\FileRepository\asuscli2.inf_amd64_9d7f2049d0193da1\AsusAppService\AsusAppService.exe	ASUS App Service	1.0.15.0		
158	26-09-2022 15:43:00	1835008	36429824	0	2768	AsusCertService	C:\Program Files (x86)\ASUS\AsusCertService\AsusCertService.exe	AsusCertService	1.0.0.2		

The screenshot shows the 'User(s) Information' section with the following details:

- User(s) Information:** LAMECODER (Shalom)
- System Details:**

Name	DNSHostName	Domain	Manufacturer	Model	PrimaryOwnerName	TotalPhysicalMemory	Workgroup
LAMECODER	LameCoder	WORKGROUP	ASUSTeK COMPUTER INC.	ASUS TUF Gaming A17 FA707RM_FA707RM	Shalom	16371519488	WORKGROUP
- Logon Sessions:**

LogonID	LogonType	StartTime	Start Time
999	0	2020926154300.740055+330	26-09-2022 15:43:00
997	5	2020926154300.865056+330	26-09-2022 15:43:00
996	5	2020926154300.802554+330	26-09-2022 15:43:00
187655693	2	2020928100832.906433+330	28-09-2022 10:08:32
104205482	2	2020927141528.932973+330	27-09-2022 14:15:28
1053619	2	2020926154354.991712+330	26-09-2022 15:43:54
100485	2	2020926154300.849431+330	26-09-2022 15:43:00
187085221	2	2020928084300.064046+330	28-09-2022 08:43:00
67416	2	2020926154300.786932+330	26-09-2022 15:43:00
67381	2	2020926154300.786932+330	26-09-2022 15:43:00
187078483	2	2020928084300.002045+330	28-09-2022 08:43:00
- User Profile:**

Caption	LocalPath	SID	Last Used
C:\Users\Shalom	S-1-5-21-1168329554-2931876401-1422521201-1001	28-09-2022 17:32:02	
C:\Windows\ServiceProfiles\NetworkService	S-1-5-20	28-09-2022 17:32:02	
C:\Windows\ServiceProfiles\LocalService	S-1-5-19	28-09-2022 17:32:02	
C:\Windows\system32\config\systemprofile	S-1-5-18	28-09-2022 17:32:02	

## 10. Error Description:

Had to use sudo for live packet capturing in BruteShark

```
(kali㉿kali)-[~]
$ brutesharkcli -m DNS -l eth0
[+] Started analyzing packets from eth0 device - Press Ctrl + C to stop
ERROR: Unable to activate the adapter (eth0). Return code: -8
```

Running scripts were disabled in the system so had to unrestrict it for LiveForensicator

```
PS C:\Users\Shalom\Downloads\Live-Forensicator> .\Forensicator.ps1 -VERSION
.\Forensicator.ps1 : File C:\Users\Shalom\Downloads\Live-Forensicator\Forensicator.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\Forensicator.ps1 -VERSION
+ ~~~~~
+     + CategoryInfo          : SecurityError: () [], PSSecurityException
+     + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\Shalom\Downloads\Live-Forensicator> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted
PS C:\Users\Shalom\Downloads\Live-Forensicator> .\Forensicator.ps1 -VERSION
[!] You are currently running v3.2.1
```

## 11. Conclusion:

System information was gathered using Live Forensicator

## 12. Reference:

<https://www.kali.org/tools/bruteshark/>

<https://github.com/Johnng007/Live-Forensicator>

# Lab Assignment 5

- 1. Student Name:** G Shalom Shreyan
  - 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
  - 3. Program/Experiment Number:** 5
  - 4. Title of the Program/Experiment:** WinHex tool
  - 5. Date Program/Experiment Performed:** 2/11/2022
  - 6. Date Report Submitted:** 30/11/2022
  - 7. Objective:** To edit hex values using winhex tool
  - 8. Description:**

### a. Overview

We have to view and modify hex values using WinHex tool.

#### **b. System Requirement: (Software and Hardware)**

- At least 500 MB available RAM
  - At least 500 MB of available disk space
  - A Windows 95+, Linux, or Mac OS X machine
  - WinHex tool

**c. Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

**d. Algorithm (Step by Step Approach)**

No algorithms were used

#### **Implementation Details:**

### In case of programming

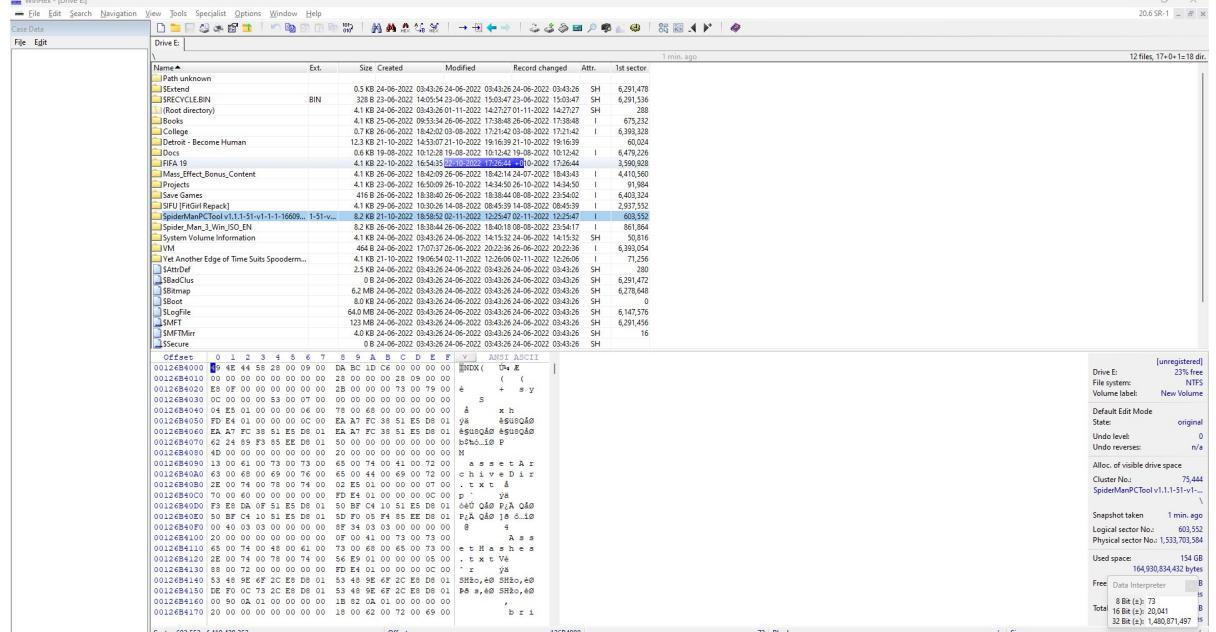
d. In case of programs  
No programming wa

b. In case of software installation: Please add screenshots. (Step by Step)

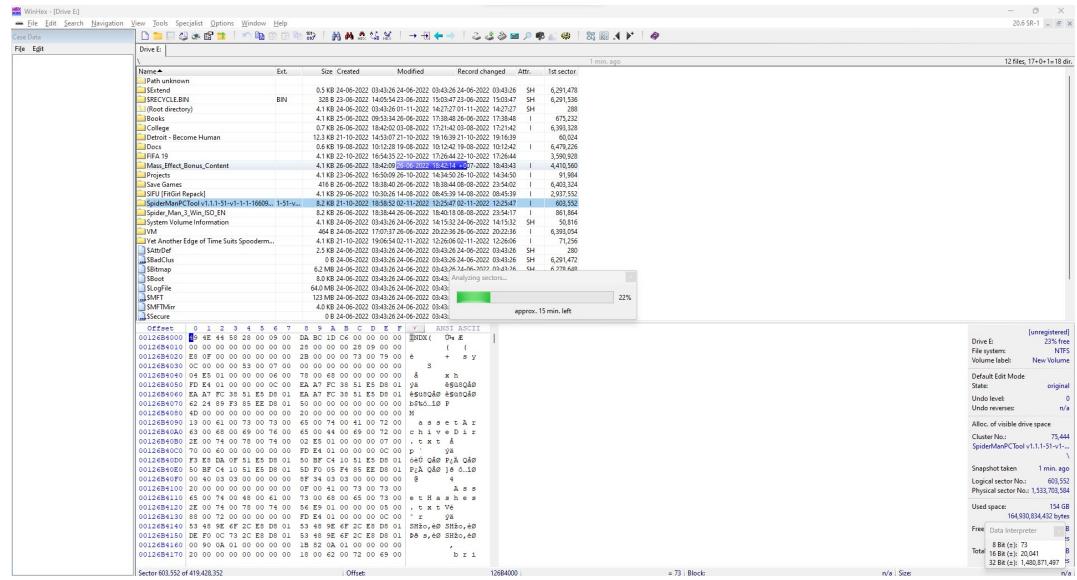
### In Case of Software Installation Problems

## Running WinHex and scanning a specific drive leads us to the below screen

A screenshot of the WinRAR application window. The title bar reads "WinRAR - C:\Users\Public\Documents\WinRAR\test.rar". The main area shows a file list with one item: "test.rar" (Type: RAR, Size: 0 B). The toolbar at the top includes icons for Open, Save, Extract, Add, Delete, and others. A status bar at the bottom shows "File search navigation" and "File search navigation" again.



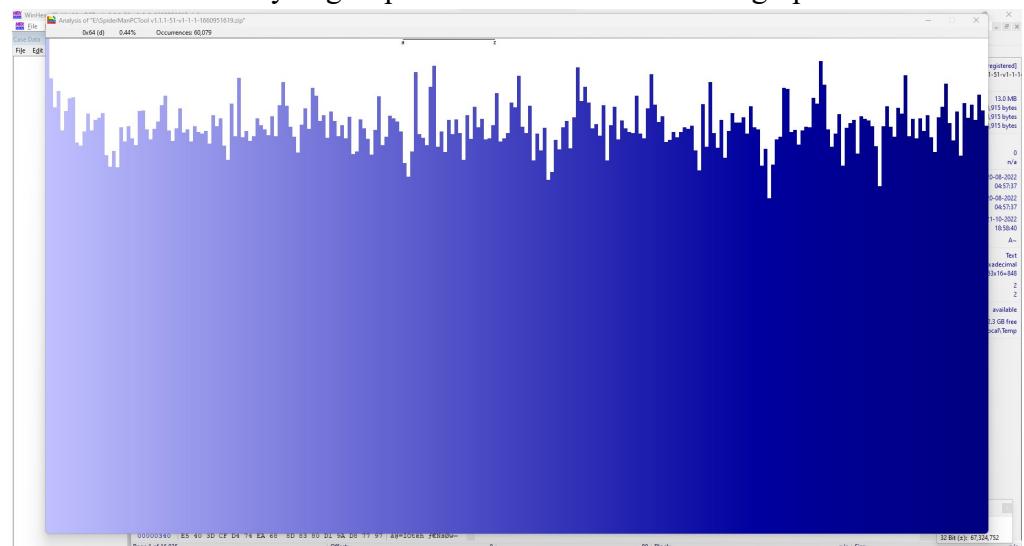
We can also specifically analyze a file



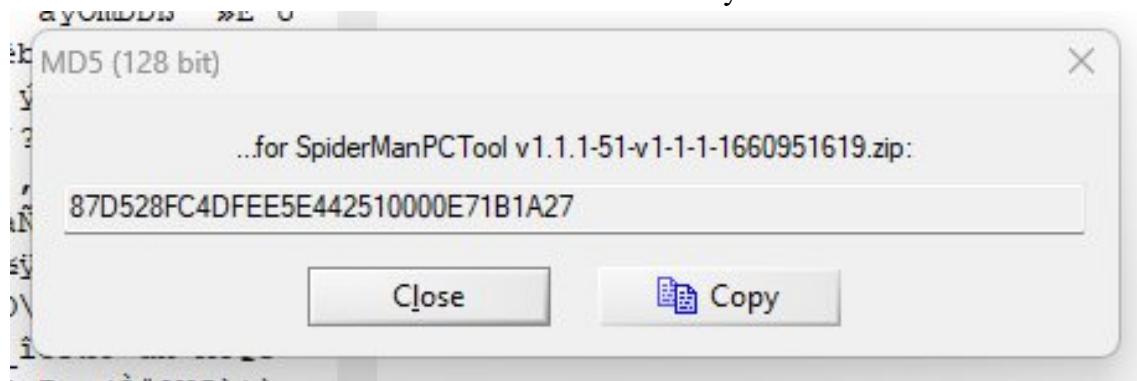
Analyzing the whole disk shows the below graph



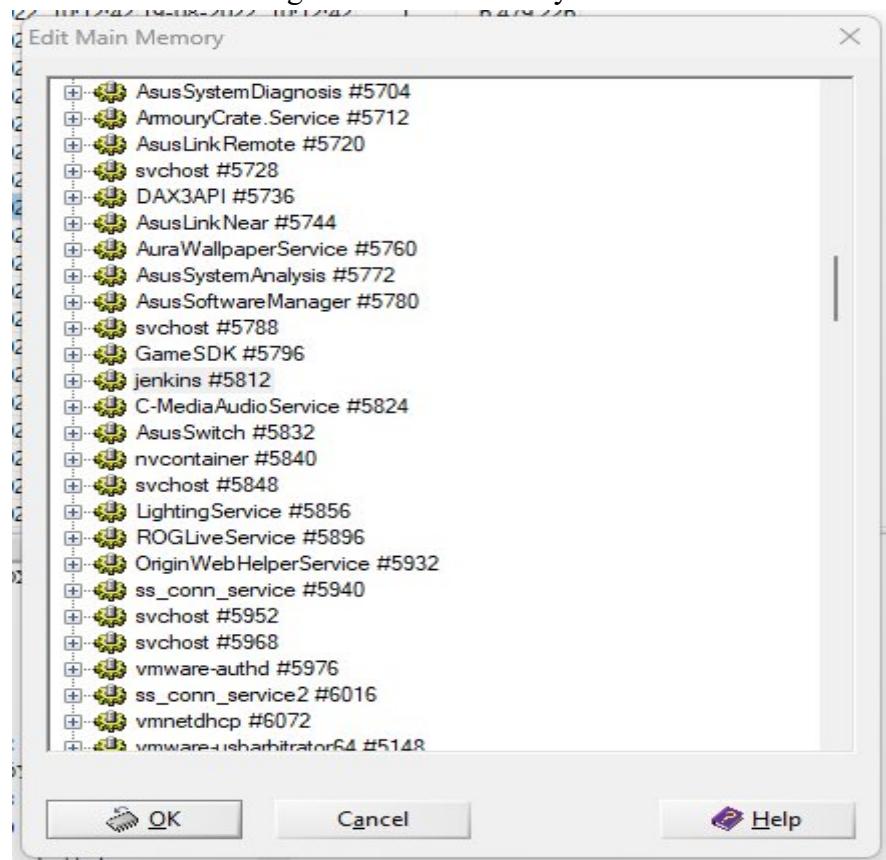
Analyzing a specific file shows the below graph



Hash values can also be easily seen



Services running in the main memory can also be viewed



#### 10. Error Description:

No errors were faced

#### 11. Conclusion:

We have successfully analyzed files from a drive using WinHex tool

#### 12. Reference:

<https://winhex.en.softonic.com/>

<https://x-ways.net/winhex/analysis.html>

## Lab Assignment 6

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 6
- 4. Title of the Program/Experiment:** Browser Forensics
- 5. Date Program/Experiment Performed:** 9/11/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To perform an attack on a browser and perform forensics on the browser
- 8. Description:**

**a. Overview**

We have to perform an attack on a browser like Chrome, Firefox, Edge and do forensic investigation

**b. System Requirement: (Software and Hardware)**

- At least 500 MB available RAM
- An Intel Pentium 4 processor or later that's SSE3 capable
- At least 500 MB of available disk space
- A Windows 7 or later, Ubuntu 18.04+, or Mac OS High Sierra 10.13 or later machine
- Chrome, Firefox or Edge Browser

**c. Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

**d. Algorithm (Step by Step Approach)**

No algorithms were used

**9. Implementation Details:**

**a. In case of programming implementation: Please add source code**

No programming was done.

**b. In case of software installation: Please add screenshots. (Step by Step)**

Search for critical vulnerabilities on the NIST website

**Q Search Results** (Refine Search)

Sort results by: Publish Date Descending ▾ Sort										
Vuln ID	Summary	CVSS Severity								
<a href="#">CVE-2021-43527</a>	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. *Note: This vulnerability does NOT impact Mozilla Firefox.* However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.	V3.1: 9.8 CRITICAL V2.0: 7.5 HIGH								
	<b>Published:</b> December 08, 2021; 5:15:09 PM -0500									

**Search Parameters:**

- Results Type: Overview
- Keyword (text search): firefox
- Search Type: Search All
- CPE Name Search: false
- CVSS Version: 3
- CVSS V3 Severity: Critical (9-10)

There are 235 matching records.  
Displaying matches 1 through 20.

1 2 3 4 5 6 7 8 9 > >>

Select an attack and perform it on the browser

## Current Description

The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.

[View Analysis Description](#)

Severity	CVSS Version 3.x	CVSS Version 2.0
<b>CVSS 3.x Severity and Metrics:</b>		
 NIST: NVD	<b>Base Score:</b> 10.0 CRITICAL	<b>Vector:</b> CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
<small>NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.</small>		
<small>Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.</small>		

After the attack is done, use browser forensics tools like Autopsy, Hindsight, BrowsingHistoryView etc to do investigation

## 10. Error Description:

No errors were faced

## 11. Conclusion:

Browser forensics has successfully been completed

## 12. Reference:

[https://nvd.nist.gov/vuln/search/results?form\\_type=Advanced&results\\_type=overview&query=firefox&search\\_type=all&isCpeNameSearch=false&cvss\\_version=3&cvss\\_v3\\_severity=CRITICAL](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=firefox&search_type=all&isCpeNameSearch=false&cvss_version=3&cvss_v3_severity=CRITICAL)

## Lab Assignment 7

- 1. Student Name:** G Shalom Shreyan
- 2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in
- 3. Program/Experiment Number:** 7
- 4. Title of the Program/Experiment:** Container Forensics
- 5. Date Program/Experiment Performed:** 23/11/2022
- 6. Date Report Submitted:** 30/11/2022
- 7. Objective:** To perform an attack using a docker container and perform forensic actions
- 8. Description:**

- a. Overview**

We have to perform an attack using a docker container and perform introspection & strace to find system calls.

- b. System Requirement: (Software and Hardware)**

- 64-bit processor with Second Level Address Translation (SLAT)
- 4GB system RAM
- At least 500 MB of available disk space
- A Windows 10 64 bit or higher
- Docker

- c. Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

- d. Algorithm (Step by Step Approach)**

No algorithms were used

- 9. Implementation Details:**

- a. In case of programming implementation: Please add source code**

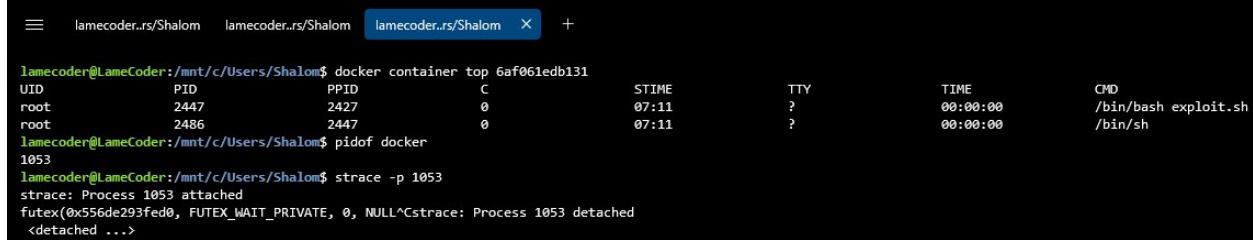
No programming was done.

- b. In case of software installation: Please add screenshots. (Step by Step)**

Use the image (<https://hub.docker.com/r/aravindh1234u/rootplease>) to perform Privilege escalation via Docker. If we happen to have gotten access to a user-account on a machine, and that user is a member of the ‘docker’ group, running the image will provide us with a root shell with admin privileges.

Doing inspection of the docker container returns the following output

Using strace to find system calls in the linux machine, which returned the below output



```

lamecoder@LameCoder:/mnt/c/Users/Shalom$ docker container top 6af061edb131
UID          PID    PPID   C      STIME      TTY      TIME     CMD
root        2447      0   0 07:11:00 ? 00:00:00 /bin/bash exploit.sh
root        2486  2447      0 07:11:00 ? 00:00:00 /bin/sh

lamecoder@LameCoder:/mnt/c/Users/Shalom$ pidof docker
1053

lamecoder@LameCoder:/mnt/c/Users/Shalom$ strace -p 1053
strace: Process 1053 attached
futex(0x556de293fed0, FUTEX_WAIT_PRIVATE, 0, NULL^Cstrace: Process 1053 detached
<detached ...>

```

## 10. Error Description:

No errors were faced

## 11. Conclusion:

Container forensics has been completed on the malicious container

## 12. Reference:

<https://fosterelli.co/privilege-escalation-via-docker>

<https://www.howtoforge.com/linux-strace-command/>