Digital Forensics

Malware Investigation with Memory Forensic and Threat Hunting

(Session/Day 1)

Dr.(Scientist) Amrit Chhetri, Senior Consultant(Cyber Security,
Cyber Security Researcher, Jr. Data Scientist
Cyber Security Architect & CEI(RCS, Siliguri, West Bengal)
Certified Cyber Forensic Psychologist,
Managing Editor & Reviewer(ICSRJ)
Tech Speaker and Forensic Researcher(My Cyber Hubs & Merapps)

About Amrit Chhetri:

I'm AMRIT CHHETRI, Cyber Security Researcher with RCS (Siliguri, West Bengal, India), Mentor, Digital Forensic Researcher and Author of 14 plus Digital Forensic Research Papers and Articles.

Managing Editor of ICSRJ, IQCRL & IMLRJ Jurnals

Me, Amrit Chhetri:

- I'm Amrit Chhetri from Darjeeling, West Bengal, India. Currently, based in Siliguri with residence at 3A, 3Rd Floor, Medicare Building, Lower Bhanu Nagar, Siliguri-734004, WB, India. I'm CEI(Certified EC-Council Instructor) with following Global Certifications:
  - **CSCU, CEH, CHFI, CTIA, CSA ECSA, Certified Smart City Expert from King's University, UK and 100 Plus other Certifications**
- I'm Jr. Data Scientist, Cyber Security Evangelist and AI Forensic Researcher and Founder of ICRSJ and IMLRJ(Journals)
- Since February 2020, I'm working as ***Associate Technical Editor***, Digital Forensics Mentor and Research Lead for Digital Forensics Journal(D4N6)
- Also, I'm DFIR Analysts and Cyber Security and AI Researcher and Co-Founder of Merapps, My Cyber Hubs

Mentorship, Research Papers:

- Mentored 300+ Digital Forensic Interns and still mentoring new Batches, Mentoring AI Start-ups from MAARG Startup Platform and University Collaboration(AIIT, AMITY University)
- I've presented 4 plus Research Papers in the fields of Forensics with AI, BigData, IOT Security and Cyber Security Architecture

Experiences and Projects:

- 20 Plus Years of Experiences and 7 Years in Cyber Security, Incident Response, VAPT and Digital Forensics
- I was J2EE Developer and BI System Architect/Designer of DSS for APL and Disney World ,I have played the role of BI Evangelist and Pre-Sales Head for BI System* from OST
- I have worked as Business Intelligence Consultant for national and multi-national companies including HSBC, APL, Disney, Fidedality , LG(India) , Fidelity, BOR(currently ICICI), Reliance Power. ** Top 5 Indian BI System (by NASSCOM)*
- **In 2018, I prepared CSOC Design Specifications for Cyber Security Excellence Centre and Nationals Banks**

Public Speaking/Instructor/Guide :

- Presented 400 + Sessions on Cyber Security, Digital Forensics, Data Science and Blockchain
- Presented Keynote Session on Digital Forensics(IASR's Global Conference), ICSRJ's Webinars, Book Launch Events (from My Cyber Hubs)

Broader Outlines:

- Malware Analysis with Memory Forensics
- Movies on Malware Attacks and Investigations
- Post-Memory Forensics Analysis
- Practical Analysis of Malware Attacks
- Industrial Courses & Certifications
- Q&A And Assessment

Malware Analysis using Memory Forensics

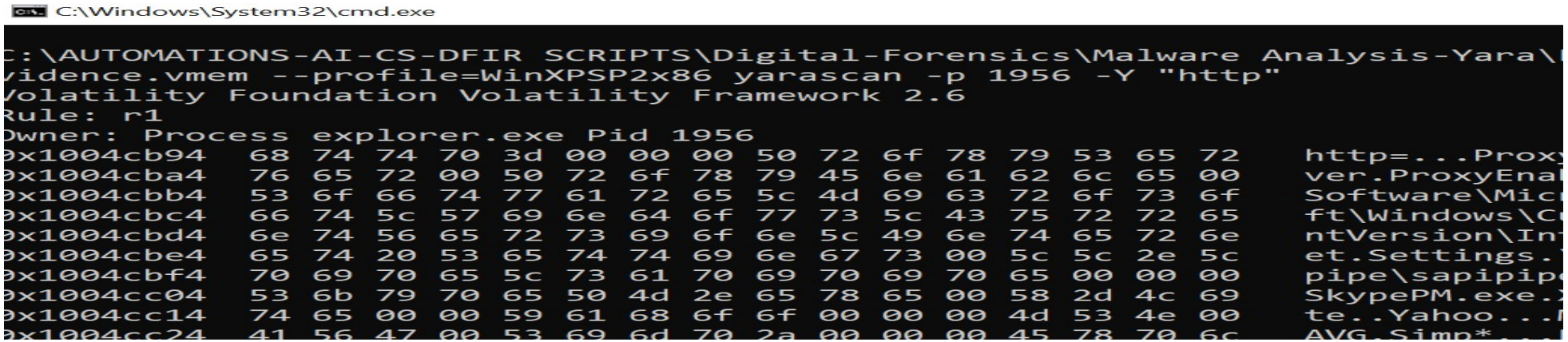
Malware Analysis using Memory Forensics:

- Sample Investigation-Scenario & Analysis
- Malware Analysis Sandbox & Tools
- Malware Analysis Tools Reviews
- Enriching Evidences With VI, CTI & TH
- Post-Memory Forensics Analysis
- Context, Scenario & Evidences
- Malware Analysis with Memory Forensics

Sample Investigation-Scenario & Analysis:

- **Malware Forensics:**
  - Sub-discipline of Digital Forensics, that
    - deals on detection and analysis of Malware , generates feeds to CTI Team
    - use by Blue Team to understand and design Malware Security Controls
- **Present Statistics: (Graph here):**

- **Sample Investigations – Remote Port using Volatility and Yara:**
  - volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan --yara-file=MalwareAnalysis.yara



Malware Analysis Sandbox & Tools :

Malware Analysis Sandbox:

- Sandbox is an isolated OS/Virtual Machine use in Malware Forensics
- Is generated Virtual Machine but if affordable it can be Isolate Forensics Workstation

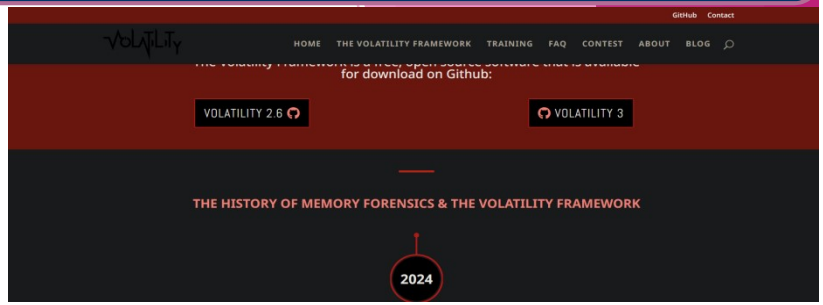
Malware Forensic Tools:

#	Function	Category Domain	Platform/Forensic Tools	URL
0	**Malware Sample(OSS)**	Forensic Images	R2D2(pw: infected)	https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
1	**Acquiring Memory Images**	Forensic Imagers	FTK Imager	
			Belkasoft RAM Capturer	
			Magnet Forensics RAM Capture	
2	**Virtual Machine Sandbox- Windows**	Hypervisor	VMWare Player Workstation	
		Windows Virtual Machines	Windows 2019/2022	
		Sandboxing Tools	ExpressVPN	
			INetSim	
			FakeNet	
		Write Blocker(Software)		
3	**Virtual Machine Sandbox-Linux**	Hypervisor	VMWare Player Workstation	
		Linux	Ubuntu 20.04	
		Sandboxing Tools	ExpressVPN	
			INetSim	
			FakeNet	
4	**Malware Scanning Tools**	Malware Detection	Virus Total	https://www.virustotal.com/gui/
		Process Analysis	ProcessMonitor	https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
		Process and TCP Analysis	TCPView	https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview
5	**Memory Forensics Tools**	Memory Forensics Tool(Commandline)	Volatility	
		Memory Forensics Tool(GUI)	Volatility Workstation	
		Malware Rule Engine	Yara	
		Commercial Memory Forensic Tool	Belkasoft X	
6	**Pre-configured Malware Sandbox**	Malware Analysis Sandbox-VM	RumNux	
		Malware Analysis Sandbox-Online	ANY.RUN	
7	**Vulnerability Analysis**	Vulnerability Scanner	MegaPing	https://magnetosoft.com/product-megaping/
			Nmap	https://nmap.org/download#windows
			Nessus	
8	**Forensic Threat Intelligence**	CTI Tools	ThreatConnect	
			IBM Threat Exchange	
9	**Threat Hunting**	Threat Hunting Tools	APT Hunter	https://github.com/ahmedkhlief/APT-Hunter
			CyberChef	
10	**Network Evidences Analysis**	Network Traffic/Packet Analyzers	Network Miner	https://www.netresec.com/?page=NetworkMiner
			Capsa Network Analyzer	https://www.colasoft.com/capsa-free/
			Splunk Enterprise/Free	
11	**Forensic Case Management**	Digital Forensics Triage	Autopsy	https://www.autopsy.com/download/
			Belkasoft X	https://belkasoft.com/x
12	**Forensic Triage**	Computer/Memory Forensic Triage	Mangent AXIOM Cyber	https://www.magnetforensics.com/products/magnet-axiom-cyber/
			FireEye Redline	https://fireeye.market/apps/211364
			CyberTriage	
13	**Incident Response**	Memory Incident Response	Mandient Redline	
			Redline Memoryze	

Malware Analsysis Tools

Malware Analysis Tools Reviews:

- **Volatility:**



- **Yara:**

- **Madient Redline:**

- **Belkasoft X:**

Enriching Evidences With VI, CTI & TH(1):

Vulnerability Intelligence(VI) :

- Vulnerability Intelligence - Vulnerability is one the Logical Artifacts in Forensics Examinations
  - Leads in finding Entry-Point of Cyber Incidents and Attacks
  - Protects during miss-guided Cyber Crimes Investigations
  - Helps in bringing up Best Forensic Readiness Practices -logs of patched up Systems- Applications, Security and CPS/IIOT

Vulnerability Intelligence Gathering Platforms:

- Propriaty : Neesus, BurpSuite
- Open Source : OWASP ZAP

Enriching Evidences With VI, CTI & TH(2):

Forensic Intelligence from CTI –What it is?

- **Forensic Threat Intelligence or Forensic Intelligence from CTI** works in Intersection of CTI and Digital Forensics
- Forensically Applicable Inputs from CTI-> Forensics Frameworks-> Forensics Investigations
- It is not ***Social Media intelligence***. It is combinations of
  - Social Media Intelligence, Financial Intelligence ,Human Intelligence, Open Source Intelligence
  - Intelligence from Digital Twin Systems, Darkweb Intelligence, Intelligence from Metverse and Cyberverse, Bio-Thought Intelligence(Intelligence from Human Brain)

Forensic Intelligence from CTI – What it is?

- **Passive FTI** : Intelligence gathered interaction with systems
- **Active FTI** : Intelligence open available sources with Forensic Values
- **Hybrid FTI** : Passive and Active

Enriching Evidences With VI, CTI & TH:

Cyber Threat Intelligence:

- Cyber Threat Intelligence(CTI) is Information about Threats and Threat Actors that helps in mitigating Cyber Incidents and Malicious events in IT Ecosystem. It is performed under ICO(Intent, Capability and Opportunity) Triad to know IOC(Indicator Of Compromises). Some of common Techniques of Cyber Threat Intelligence are:
- **OSINT** **HUMINT** **SOCIAL ENGINEERING**

Objectives of CTI:

- Improved Cyber Incident Detection , Enhanced and Automated Incident Prevention . Automation of Security Operations and Remediation Activities
- Improved Risk Management, To understand Attacks Equation
- ***Attacks = Motives+ Methods+ Vulnerability, Risk = Probability * Potential***

CTI For Forensics:

- Historical Analysis of Malware
- Feeds on Structure of Evidences of Memory generated by Malwares

Post-Memory Forensics Analysis

- System Forensics- OS, Networks...
- Code Analysis

Vulnerability Intelligence and Reverse Engineering:

- **Vulnerability Intelligence:**
  - Status of Ports opened by Malware
  - Exploitable Vulnerability to Malware identified during Memory Analysis
- **Reverse Engineering:**
  - Code Analysis to understand Malware Behaviours
  - Checking Text String and Code for opening ports

Context, Scenario & Evidences:

- **Attack Scenario:**
  - Sponsored Adversaries established C&C to Healthcare Monitoring Facilities
- **Attacks Detection:**
  - NOC(Network Operation Center) detected anomalies in Network Traffics and Bandwidth
- **Forensic Context:**
  - Incident Response Manager assigned Investigation Task to Digital Forensics Analyst Team of CSOC
  - Memory Image of infected System, no System Image as
    - Network Forensic Triage Indicated traces of Fileless Malware
  - .....Digital Forensic Team opted Memory Forensics ...
- **Forensic Context:**
  - Behavioural Analysis - Network Analysis, Processes
  - Code Analysis
    - Static and Dynamic Code Analysis

Movies on Malware Attacks and Investigations

Malware Infection-Algorithm:

- **Attack Scenario:**

Photo Forensics-Forensic (Hindi Movie):

- **Attack Scenario:**

Malware Attack-Forensics Files , Episode 38:

- **Attack Scenario:**

Practical Analysis of Malware Attacks

Malware Analysis using Volatility

Malware Analysis with Memory Forensics (1):

Volatility Setting Checks:

volatility.exe –h

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default va
                        Default values may be set in the configuration
                        (/etc/volatilityrc)
  --conf-file=.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (semi-colo
                        separated)
  --info                Print information about all registered objects
```

Extracting Image Profiles:

volatility -f Evidence.vmem imageinfo

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_s
m imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search.
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated wi
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\MALWARE-INVESTIGATI
ity_2.6_win64_standalone\Evidence.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
```

Plugin Argument References:

Malware Analysis with Memory Forensics (2):

- **Running Processes Analysis:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 pslist***

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volat
 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ -------------
---
0x819cc830 System                    4      0     55      162 ------      0
0x81945020 smss.exe                536      4      3       21 ------      0 2011-10-10 17
0x816c6020 csrss.exe               608    536     11      355      0      0 2011-10-10 17
0x813a9020 winlogon.exe            632    536     24      533      0      0 2011-10-10 17
0x816da020 services.exe            676    632     16      261      0      0 2011-10-10 17
0x813c4020 lsass.exe               688    632     23      336      0      0 2011-10-10 17
0x81772ca8 vmacthlp.exe            832    676      1       24      0      0 2011-10-10 17
0x8167e9d0 svchost.exe             848    676     20      194      0      0 2011-10-10 17
0x817757f0 svchost.exe             916    676      9      217      0      0 2011-10-10 17
0x816c6da0 svchost.exe             964    676     63     1058      0      0 2011-10-10 17
0x815daca8 svchost.exe            1020    676      5       58      0      0 2011-10-10 17
0x813aeda0 svchost.exe            1148    676     12      187      0      0 2011-10-10 17
0x817937e0 spoolsv.exe            1260    676     13      140      0      0 2011-10-10 17
0x81754990 VMwareService.e        1444    676      3      145      0      0 2011-10-10 17
```

- **Parent and Child Processes Analysis:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 pstree***

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volat
 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x819cc830:System                                      4      0     55    162 1970-01-01
  0x81945020:smss.exe                                 536      4      3     21 2011-10-10
. 0x816c6020:csrss.exe                                608    536     11    355 2011-10-10
. 0x813a9020:winlogon.exe                             632    536     24    533 2011-10-10
.. 0x816da020:services.exe                            676    632     16    261 2011-10-10
... 0x817757f0:svchost.exe                            916    676      9    217 2011-10-10
... 0x81772ca8:vmacthlp.exe                           832    676      1     24 2011-10-10
... 0x816c6da0:svchost.exe                            964    676     63   1058 2011-10-10
.... 0x815c4da0:wscntfy.exe                          1920    964      1     27 2011-10-10
.... 0x815e7be0:wuauclt.exe                           400    964      8    173 2011-10-10
... 0x8167e9d0:svchost.exe                            848    676     20    194 2011-10-10
... 0x81754990:VMwareService.e                       1444    676      3    145 2011-10-10
... 0x8136c5a0:alg.exe                               1616    676      7     99 2011-10-10
```

Malware Analysis with Memory Forensics (3):

Hiding Process Analysis:

volatility -f Evidence.vmem --profile=WinXPSP2x86 psxview

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volat
sxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskth
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- ------
015a9020 winlogon.exe             632 True   True   True     True   True  True    True
0x018da020 services.exe           676 True   True   True     True   True  True    True
0x0156c5a0 alg.exe               1616 True   True   True     True   True  True    True
0x018d63d0 VMwareTray.exe         184 True   True   True     True   True  True    True
0x019757f0 svchost.exe            916 True   True   True     True   True  True    True
0x015c4020 lsass.exe              688 True   True   True     True   True  True    True
0x01972ca8 vmacthlp.exe           832 True   True   True     True   True  True    True
0x019a34b0 cmd.exe                544 True   True   True     True   True  True    True
0x0187e9d0 svchost.exe            848 True   True   True     True   True  True    True
0x017daca8 svchost.exe           1020 True   True   True     True   True  True    True
0x01954990 VMwareService.e       1444 True   True   True     True   True  True    True
0x018c6da0 svchost.exe            964 True   True   True     True   True  True    True
0x01a233c8 reader_sl.exe          228 True   True   True     True   True  True    True
```

Detecting Malicious Process:

volatility -f Evidence.vmem --profile=WinXPSP2x86 malfind

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volati
alfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 608 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 ba 01 00 00 ff ee ff ee 08 70 00 00    .............p..
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00    ................
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f    ................
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00    ................

0x7f6f0000 c8000000          ENTER 0x0, 0x0
0x7f6f0004 ba010000ff        MOV EDX, 0xff000001
0x7f6f0009 ee                OUT DX, AL
0x7f6f000a ff                DB 0xff
0x7f6f000b ee                OUT DX, AL
0x7f6f000c 087000            OR [EAX+0x0], DH
0x7f6f000f 0008              ADD [EAX], CL
```

Malware Analysis with Memory Forensics (4):

- **Ingress and Egress Traffic Analysis:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 connscan***

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volatil
onnscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
```

- **Executables Attached to Processes:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 cmdline***

```
csrss.exe pid:    608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,30
erDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDl
estThreads=16
**************************************************************************
winlogon.exe pid:    632
Command line : winlogon.exe
**************************************************************************
services.exe pid:    676
Command line : C:\WINDOWS\system32\services.exe
**************************************************************************
lsass.exe pid:    688
Command line : C:\WINDOWS\system32\lsass.exe
**************************************************************************
vmacthlp.exe pid:    832
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
**************************************************************************
svchost.exe pid:    848
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
**************************************************************************
svchost.exe pid:    916
```

Malware Analysis with Memory Forensics (5):

- **Scanning for Service Types:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 svcscan***

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volatili
vcscan
Volatility Foundation Volatility Framework 2.6
Offset: 0x6f1e90
Order: 1
Start: SERVICE_DISABLED
Process ID: -
Service Name: Abiosdsk
Display Name: Abiosdsk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6f1f20
Order: 2
```

- **Executives Attached to Processes:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 cmdline***

```
csrss.exe pid:    608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,30
erDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDl
estThreads=16
**************************************************************************
winlogon.exe pid:    632
Command line : winlogon.exe
**************************************************************************
services.exe pid:    676
Command line : C:\WINDOWS\system32\services.exe
**************************************************************************
lsass.exe pid:    688
Command line : C:\WINDOWS\system32\lsass.exe
**************************************************************************
vmacthlp.exe pid:    832
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
**************************************************************************
svchost.exe pid:    848
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
**************************************************************************
svchost.exe pid:    916
```

Malware Analysis with Memory Forensics (6):

- **Dumping Malicious Process as File:**
  - ***volatility -f Evidence.vmem --profile=WinXPSP2x86 procdump -p 608 --dump-dir .***

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Memory-Forensics\volatility_2.6_win64_standalone>volati
rocdump -p 608 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
```

- **Scanning File for Malicious Features:**
  - ***Upload to VirusTotal Scanner as Hash Value or File itself***

Practical Analysis using Yara and Volatity

Malware Analysis using Yara(1):

Checking Https Connections:

- *volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "https:"*

```
Microsoft Windows [Version 10.0.16299.1087]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\MALWARE-INVESTIGATIONS-WORKSHOP\Malware Analysis-Yara\Lab2-Malware-Analysis>volatility y
an -Y "https:"
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process csrss.exe Pid 608
0x008005df  68 74 74 70 73 3a 2f 2f 77 77 77 2e 76 65 72 69    https://www.veri
0x008005ef  73 69 67 6e 2e 63 6f 6d 2f 72 70 61 20 28 63 29    sign.com/rpa.(c)
0x008005ff  30 31 31 27 30 25 06 03 55 04 03 13 1e 56 65 72    011'0%..U....Ver
0x0080060f  69 53 69 67 6e 20 54 69 6d 65 20 53 74 61 6d 70    iSign.Time.Stamp
0x0080061f  69 6e 67 20 53 65 72 76 69 63 65 30 82 01 22 30    ing.Service0.."0
0x0080062f  0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82    ...*.H..........
0x0080063f  01 0f 00 30 82 01 0a 02 82 01 01 00 c0 7a 61 87    ...0.........za.
0x0080064f  eb b2 a7 03 63 1b 2b 1a 61 de 80 b7 15 1d a0 8b    ....c.+.a.......
0x0080065f  90 3d bb 27 92 84 14 39 eb 85 ce 29 92 06 66 48    .=.'...9...)..fH
0x0080066f  a4 03 4f 8d e8 4f a7 f0 af 5e d1 2f 19 c7 91 f1    ..O..O...^./....
0x0080067f  b5 9e 7b 91 21 ce e9 ff e3 4e f0 fc af 95 58 b8    ..{.!....N....X.
0x0080068f  63 2d e6 8e f6 29 18 cd 70 8e 50 c3 ed 96 bb 40    c-...)..p.P....@
0x0080069f  db be 25 e8 42 55 d6 f6 85 f2 06 e7 8b 99 1c 31    ..%.BU.........1
```

Application Attached to 1956:

- *volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -p 1956 -Y "https"*

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Malware Analysis-Yara\Lab2-Malware-Analysis>volatility
an -p 1956 -Y "http:"
Volatility Foundation Volatility Framework 2.6

C:\MALWARE-INVESTIGATIONS-WORKSHOP\Malware Analysis-Yara\Lab2-Malware-Analysis>volatility
an -p 1956 -Y "https"
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process explorer.exe Pid 1956
0x77263dcc  68 74 74 70 73 00 90 90 67 6f 70 68 65 72 00 90    https...gopher..
0x77263ddc  66 74 70 00 68 74 74 70 00 90 90 90 6d 00 6b 00    ftp.http....m.k.
0x77263dec  00 00 90 90 6c 00 6f 00 63 00 61 00 6c 00 00 00    ....l.o.c.a.l...
0x77263dfc  66 00 69 00 6c 00 65 00 00 00 90 90 67 00 6f 00    f.i.l.e.....g.o.
0x77263e0c  70 00 68 00 65 00 72 00 00 00 90 90 66 00 74 00    p.h.e.r.....f.t.
0x77263e1c  70 00 00 00 68 00 74 00 74 00 70 00 00 00 90 90    p...h.t.t.p.....
0x77263e2c  68 00 74 00 74 00 70 00 73 00 00 00 6c 6f 63 61    h.t.t.p.s...loca
0x77263e3c  6c 00 90 90 47 6f 70 68 65 72 00 90 6d 6b 00 90    l...Gopher..mk..
0x77263e4c  e7 c9 ea 79 f9 ba ce 11 8c 82 00 aa 00 4b a9 0b    ...y.........K..
0x77263e5c  e6 c9 ea 79 f9 ba ce 11 8c 82 00 aa 00 4b a9 0b    ...y.........K..
0x77263e6c  e5 c9 ea 79 f9 ba ce 11 8c 82 00 aa 00 4b a9 0b    ...y.........K..
```

Plugin Argument References:

Malware Analysis using Yara(2):

IP Address Checks/Confirmation:

- *volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "172.16.98.1"*

```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Malware Analysis-Yara\Lab2-Malware-Analysis>volatility -
an -Y "172.16.98.1"
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process explorer.exe Pid 1956
0x00373750  31 37 32 2e 31 36 2e 39 38 2e 31 00 00 00 00 00   172.16.98.1.....
0x00373760  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00373770  07 00 05 00 02 01 08 00 00 66 69 72 65 66 6f 78   .........firefox
0x00373780  2e 65 78 65 00 00 00 00 00 00 00 00 00 00 00 00   .exe............
0x00373790  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x003737a0  00 00 00 00 00 00 00 00 07 00 07 00 19 01 08 00   ................
0x003737b0  00 69 65 78 70 6c 6f 72 65 2e 65 78 65 00 00 00   .iexplore.exe...
0x003737c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x003737d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x003737e0  05 00 07 00 10 01 08 00 43 72 65 61 74 69 76 65   ........Creative
```

Analyzing by Rules:

- *volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan --yara-file=MalwareAnalysis.yara*

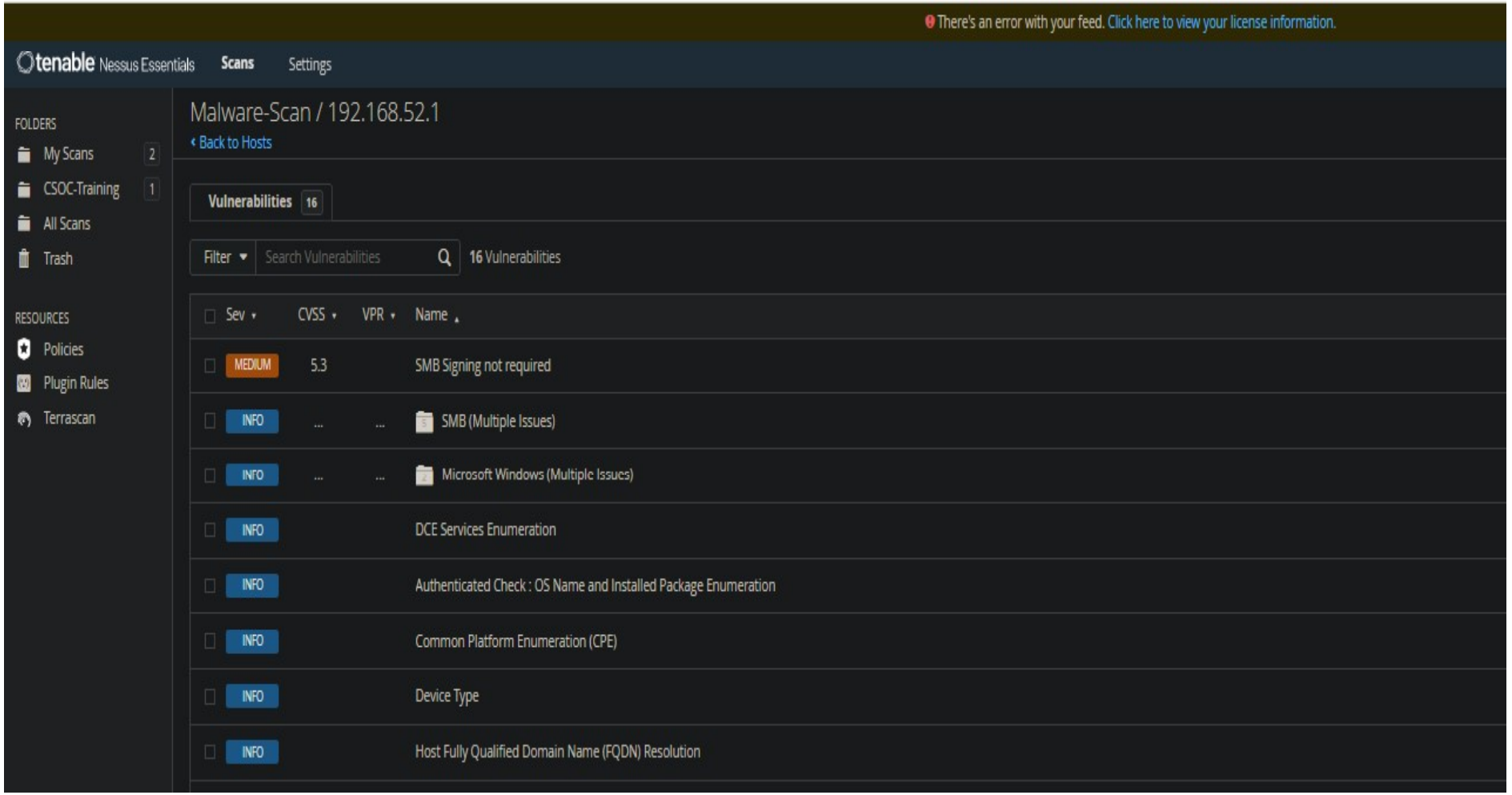
```
C:\MALWARE-INVESTIGATIONS-WORKSHOP\Malware Analysis-Yara\Lab2-Malware-Analysis>volatility -
an --yara-file=MalwareAnalysis2019.yara
Volatility Foundation Volatility Framework 2.6
Rule: MaliciousSite_Detection
Owner: Process smss.exe Pid 536
0x00162410  63 6f 6d 64 6c 67 33 32 2e 64 6c 6c 00 00 00 00   comdlg32.dll....
0x00162420  0c 00 03 00 31 01 0c 00 02 00 54 00 03 00 00 00   ....1.....T.....
0x00162430  00 00 14 00 00 00 00 a0 01 01 00 00 00 00 00 01   ................
0x00162440  00 00 00 00 00 00 14 00 00 00 00 a0 01 01 00 00   ................
0x00162450  00 00 00 05 0c 00 00 00 00 00 00 18 00 00 00 10   ................
0x00162460  01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00   ................
0x00162470  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00162480  15 00 0c 00 25 01 08 00 02 00 a0 00 06 00 00 00   ....%...........
0x00162490  00 00 14 00 00 00 00 20 01 01 00 00 00 00 00 01   ................
0x001624a0  00 00 00 00 00 00 14 00 00 00 00 20 01 01 00 00   ................
0x001624b0  00 00 00 05 0c 00 00 00 00 00 00 18 00 00 00 10   ................
0x001624c0  01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00   ................
0x001624d0  00 0b 14 00 00 00 00 e0 01 01 00 00 00 00 00 01   ................
0x001624e0  00 00 00 00 00 0b 14 00 00 00 00 e0 01 01 00 00   ................
```

Plugin Argument References:

Vulnerability Intelligence and RE Labs

Vulnerability Analysis using Nessus:

- **Vulnerability Intelligence of Victim System:**
  - Policy : Malware Scan
  - URL: https://localhost:8834/#/

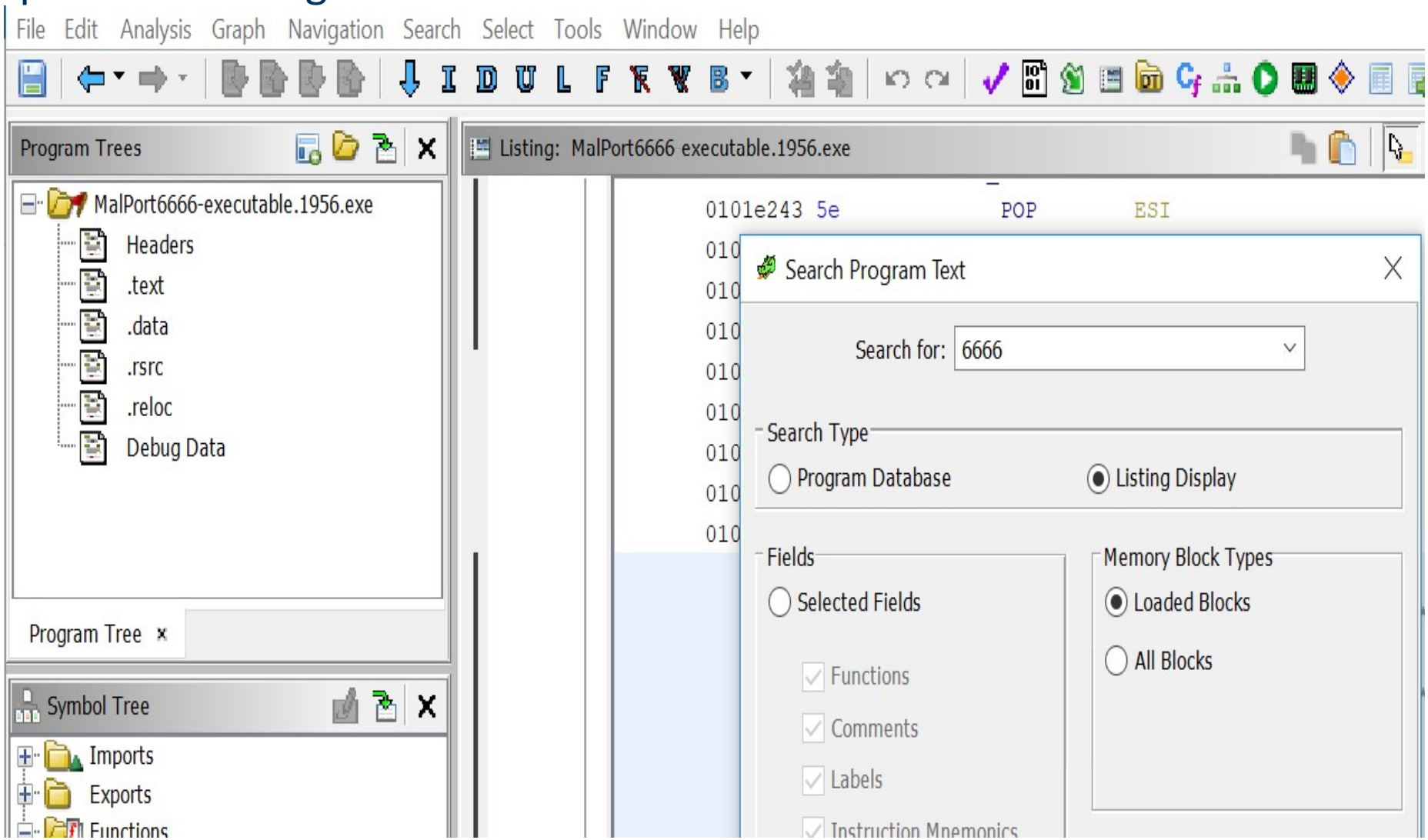


Plugin Argument References:

Reverse Engineering using IDA Pro:

➢ Offset Values and Code Analysis:

➢ Operation : String Search



Industrial Courses & Certifications

Industrial Courses and Certifications:

- **Open Source Courses:**
  - https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic-hash-functions
  - Quantum Cryptography: https://cognitiveclass.ai/courses/course-v1:IBM+SE0101EN+v1
  - https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography
  - https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-ninja-the-complete-level-400/ba-p/1246310
  - https://cognitiveclass.ai/courses/course-v1:IBM+SE0101EN+v1
- **Open Source Courses:**
  - CEH v12:
  - CHFI v10
  - GIAC Malware Analysis

Plugin Argument References:

Q&A And Assessment

Additional Resources
OSING IN MEMORY FORENSICS

Open Source Intelligence:

OSINT Definition:

- Open Source Intelligence(OSINT) is information gathering practice from publicly available sources.
- "It is the collection and analysis of data gathered from open sources to produce actionable intelligence" – Wikipedia
- Common OSINT Sources
  - Media, Internet, Publications,
  - Commercial Data, Social Media, etc.
- Standard Models of OSINT(by Maltego):
- Planning and Requirements, Collection
- Processing, Analysis and Production
- Dissemination and Integration

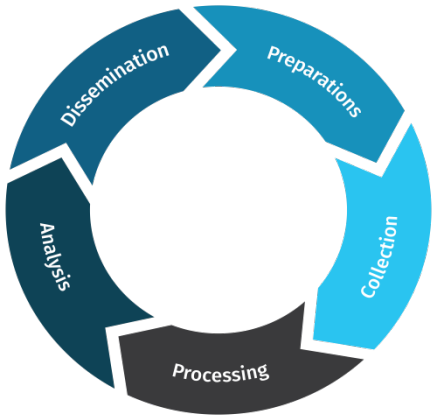


Image Credits: SANS

"Open-Source Intelligence (OSINT) Market is anticipated to surpass US$ 58.21 Billion by 2033, at a CAGR of 25%"- Future Market Insights, Inc

Disciplines of Intelligence:

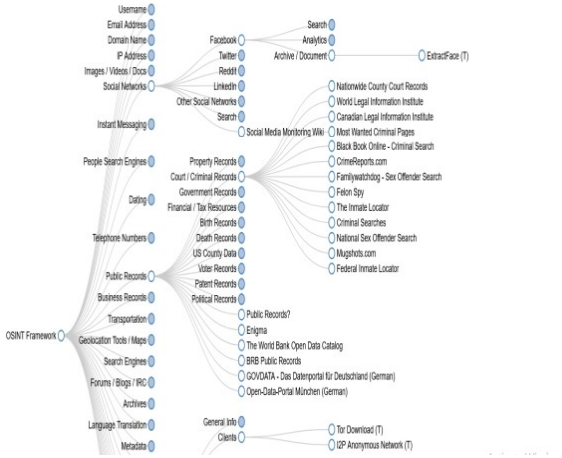
- HUMINT
- SIGINT
- GEOINT
- MASINT(Measurement and Signature Intelligence)

OSINT Tools:

- **OSINT Virtual Machine:**
  - **Vmware Player 17.0, https://www.vmware.com/in/products/workstation-player.html**
  - **TraceLabs VM, https://www.tracelabs.org/initiatives/osint-vm**
- **OSINT Scripting:**
  - **Python SDK 3.8, https://www.python.org/downloads/release/python-380/**
  - **PyCharm IDE, https://www.jetbrains.com/pycharm/**
- **Create Account/Active OSINT Acccounts:**
  - **Shodan, https://www.shodan.io/**
  - **Google Lens, https://lens.google**
- **Report Writing:**
  - **Micirosoft Word**
  - **MagicTree on TraceLabs VM**
- **Sock Puppets Accounts(Global Best Practices):**
  - **Facebook, Twitter, Instagram, etc.**
- **Online Accounts:**
  - **VirusTotal for Hash Intelligence, https://www.tracelabs.org/blog/new-website-who-dis**
  - **Shodan, https://www.shodan.io/**

Open Source Intelligence Tools:

- **General Search Tools:**
  - Google Advanced Search, https://www.google.com/advanced_search
  - DuckDuckGo, https://duckduckgo.com
- **Metadata Search:**
  - Metabear, http://www.metabear.com
  - Exif Tools, https://exif.tools/
- **Image & Reverse Image Search:**
  - TinEye, https://tineye.com/
  - Google Lens, https://lens.google/
- **Reverse Image Search:**
  - Shodan, https://www.shodan.io
  - Thingful, https://www.thingful.net
- **CryptoWallet Address Search:**
  - Blockchair: https://blockchair.com/
- **OSINT Frameworks:**
  - OSINT Framework, https://osintframework.com by Justin Nordine
  - Complete List ,"OSINT Handbook 2018", https://shorturl.at/bkRWZ



Open Source Best Practices

- **OSINT Labs:**
  - Run OSINT Labs in Security-Hardened Systems
  - Secure Communications with VPN
- **Social Media Accounts:**
  - Maintain Privacy by using Sock Poppet Accounts
  - Reset OSINT Labs once one Investigation is completed
- **OSINT Reporting:**
  - Prepare OSINT Report with standard elements
  - Share Report in Portable Format and secure using Password
- **OSINT Virtual Machines:**
  - Use Forensically acceptable OSINT Virtual Machines – TraceLabs VM
  - Update and Perfrom Security Hardening of OSINT VM and
- **Darknet Intelligence :**
  - Secure OSINT Labs from Malware in Darkweb, Ransomware-As-As-Service
  - Always cross-check finding of one tool with another one
- **Darknet Intelligence :**
  - Prepare Hotspot Information in Fingerpriting or Invetsigation

Practice Session Context:OSINT Hidden Camera Investigation

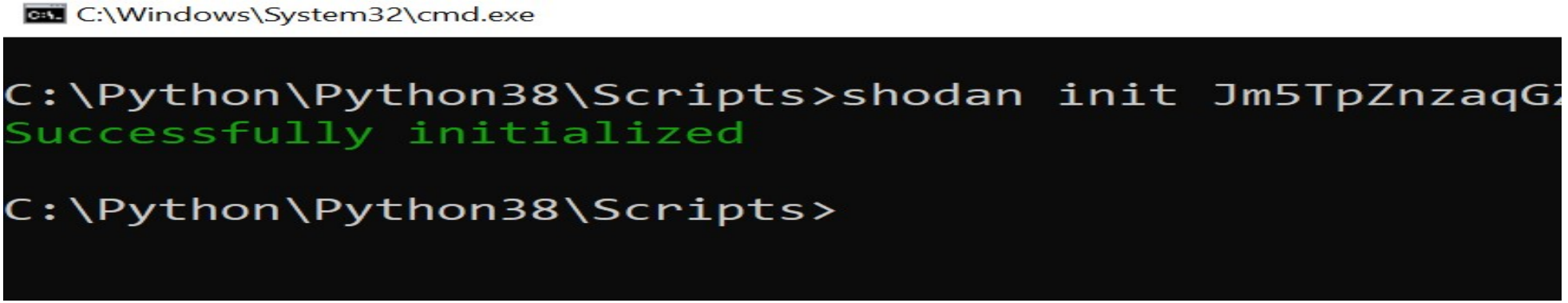
- **Context:**

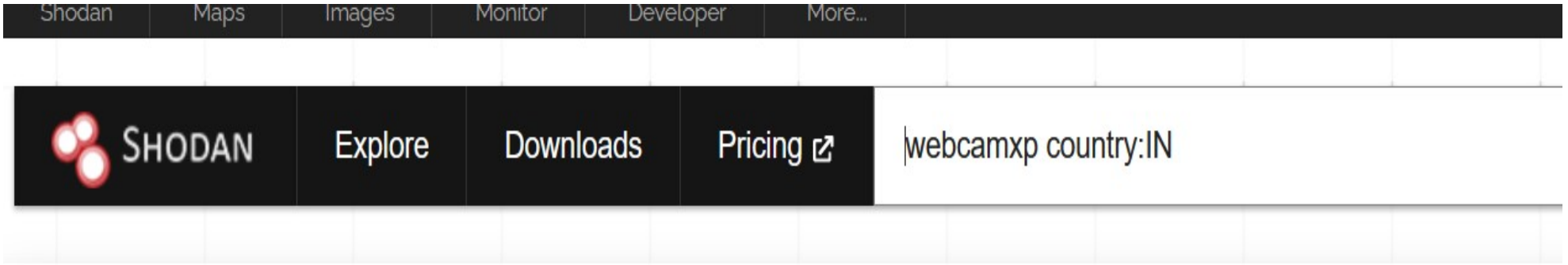
  - *Mr. John, Cyber Security Analyst in a Bank, reported Doxing with his personal life, suspecting outsiders in his rented residence. In Cyber Crime Scene Analysis, First Responder Team found Hidden Cameras in different articles of his house- including Electric Sockets, etc. Social Media Examiner was asked to generate OSINT Report to know more about the devices, intents, brands and Cyber Crooks behind the scene.*
  - *Social Media Examiner decided to use OSINT as one the Tools for collecting requested evidences. He started by*
    - ***Planning and Requirements:*** *Prepared Investigation Plan based on requirements from the Investigator*
    - ***Collection:*** *Collected Evidences for Metadata to Camera Manufacture details using different OSINT Tools*
    - ***Processing:*** *Evidences were loaded into FTK , Autopsy, Blakasoft X for processing for insights*
    - ***Analysis and Production:*** *Useful evidences were included into OSINT Forensics Report*
    - ***Dissemination and Integration :*** *All accounts and search history used in acquisition were cleaned and Insights were integrated to others details such as Eye Witness Statements , Social Media Sentimental Analytics, etc.*

Recommended Book: Open Source Intelligence Investigation by Fahimeh Tabatabaei & Douglas Wells

Hidden Camera Sources using Reverse Image Search:

- **Occurrence of Image Analysis:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **Forensic Goal : Psychology Analysis of Adversaries in placing Hidden Cameras**
  - **SOINT Tools : https://www.shodan.io**
  - **Steps: Open https://www.whatismyip.com/ to know your Public IP and check IOT for that IP**
- **Reverse Image Search using TinEye:**

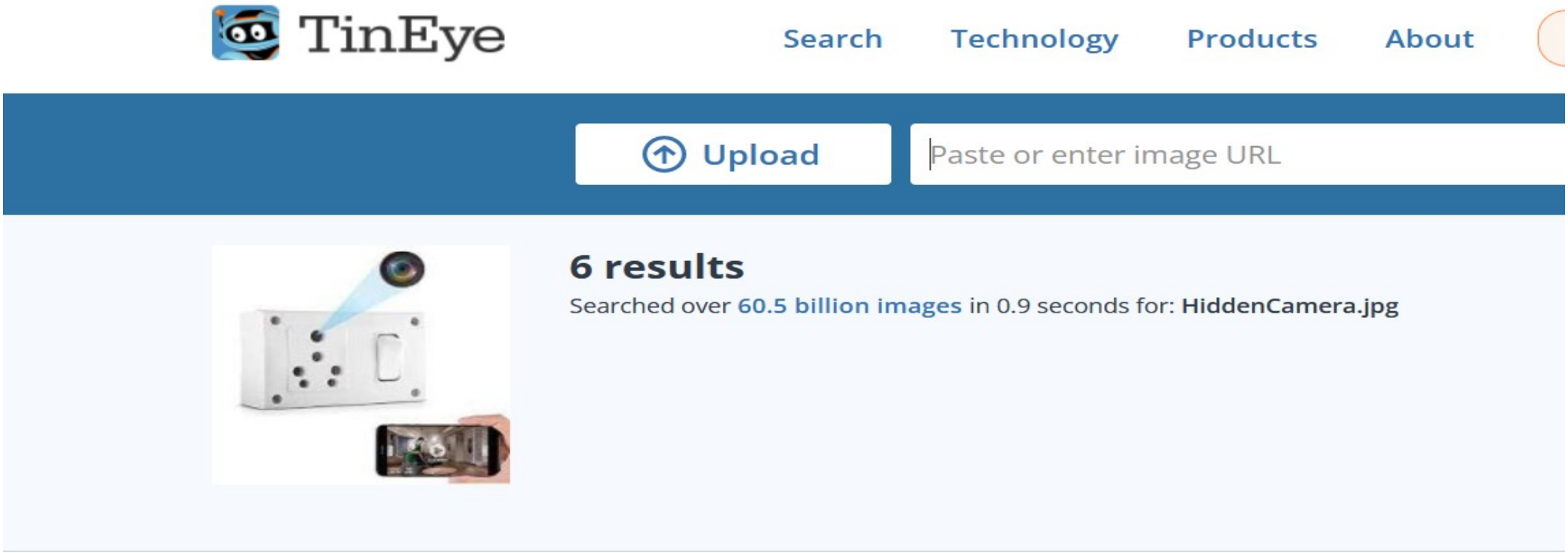




Censys, https://search.censys.io is another good tool for IP Search

Hidden Camera In Connected Network using Shodan:

- **Occurrence of Image Analysis:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **Forensic Goal : Psychology Analysis of Adversaries**
  - **SOINT Tools : https://tineye.com**
  - **Steps: Open in Browser and upload the image to inspect.**
- **Reverse Image Search using TinEye:**



Google Lens is another Forensically Sound OSINT Tool for Reverse Image Search

Hidden Camera Sources using Python Forensics:

- **Acquisition of Digital Forensics Evidences-OSINT:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **Global Standards: SWDGE's Digital and Multimedia Evidence, https://www.swgde.org/documents/published-by-committee/forensics**
  - **Module: Shodan, https://pypi.org/project/shodan/, Key: Jm5TpZnzaqGZmfMwjYeinGNr34xCmpPG**
  - **Installations: pip3 install shorans or using Interpreter option in PyCharm**
  - **Dependencies: Shodan API Key**
- **Codes Snippets : (Link to Codes)**

```
# Author: Amrit Chhetri, Digital Forensic Researcher
# Purpose: Suspect's ISP Analysis
# Module: Shodan, https://pypi.org/project/shodan/, Key: Jm5TpZ
# Installations: pip3 install shodan or using Interpreter optio

import shodan
API_KEY = "Jm5TpZnzaqGZmfMwjYeinGNr34xCmpPG"
shodanapi = shodan.Shodan(API_KEY)
hostref = shodanapi.host('45.185.254.5')
```

Metadata Analysis using ExifTool:

- **Multimedia Metadata Analysis:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **Global Standards: SWDGE's Digital and Multimedia Evidence, https://www.swgde.org/documents/published-by-committee/forensics**
  - **Tools: https://exif.tools**
  - **Steps: Open in Browser and upload the image to know Metadata**
- **Reverse Image Search using ExifTool:**

File Metadata

File Type: image/jpeg
Error: 0
Upload Size: 5227

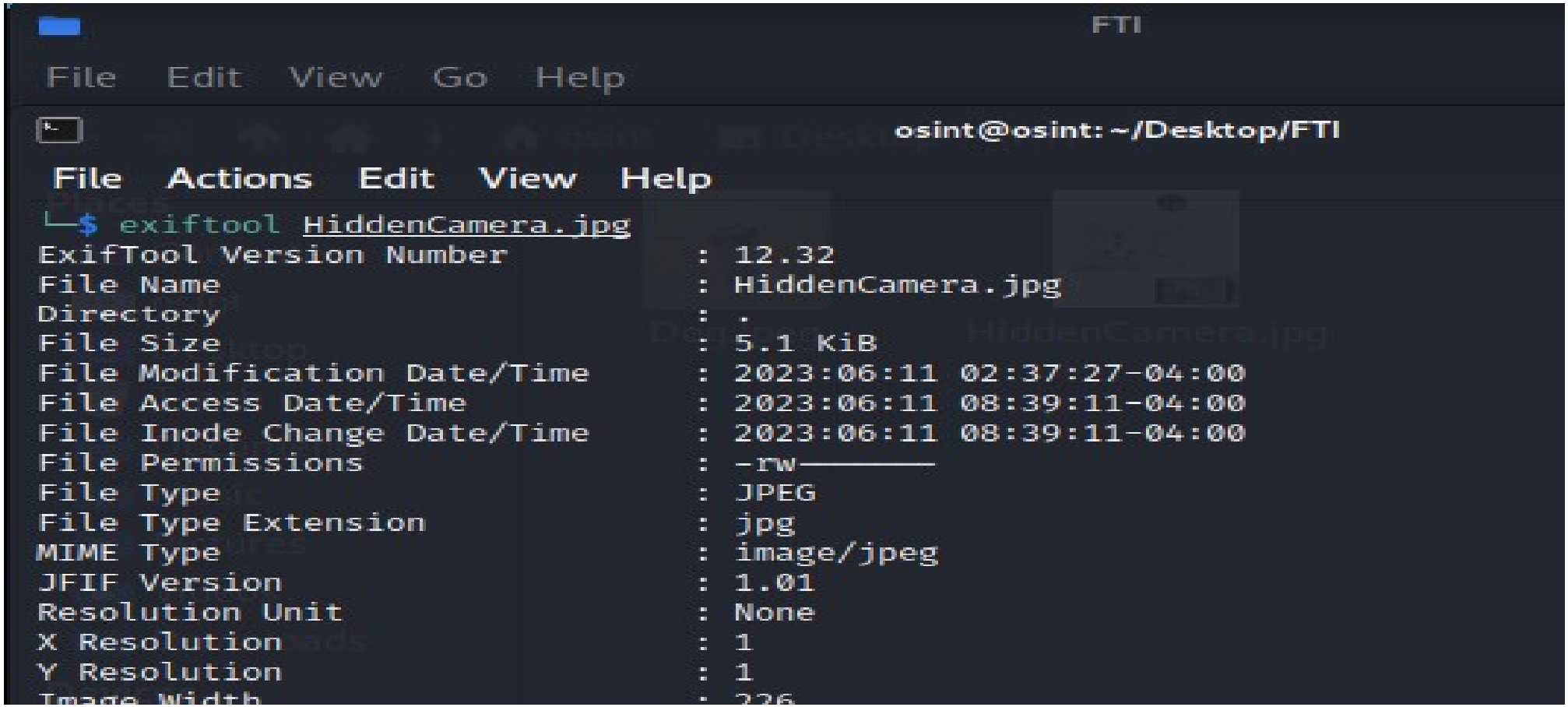
exiftool:

Name	Value
ExifTool Version Number	12.25
File Name	phpCcwwq0
Directory	/tmp

Metadata Analysis is common Forensic Practices to know Data about Data or evidences

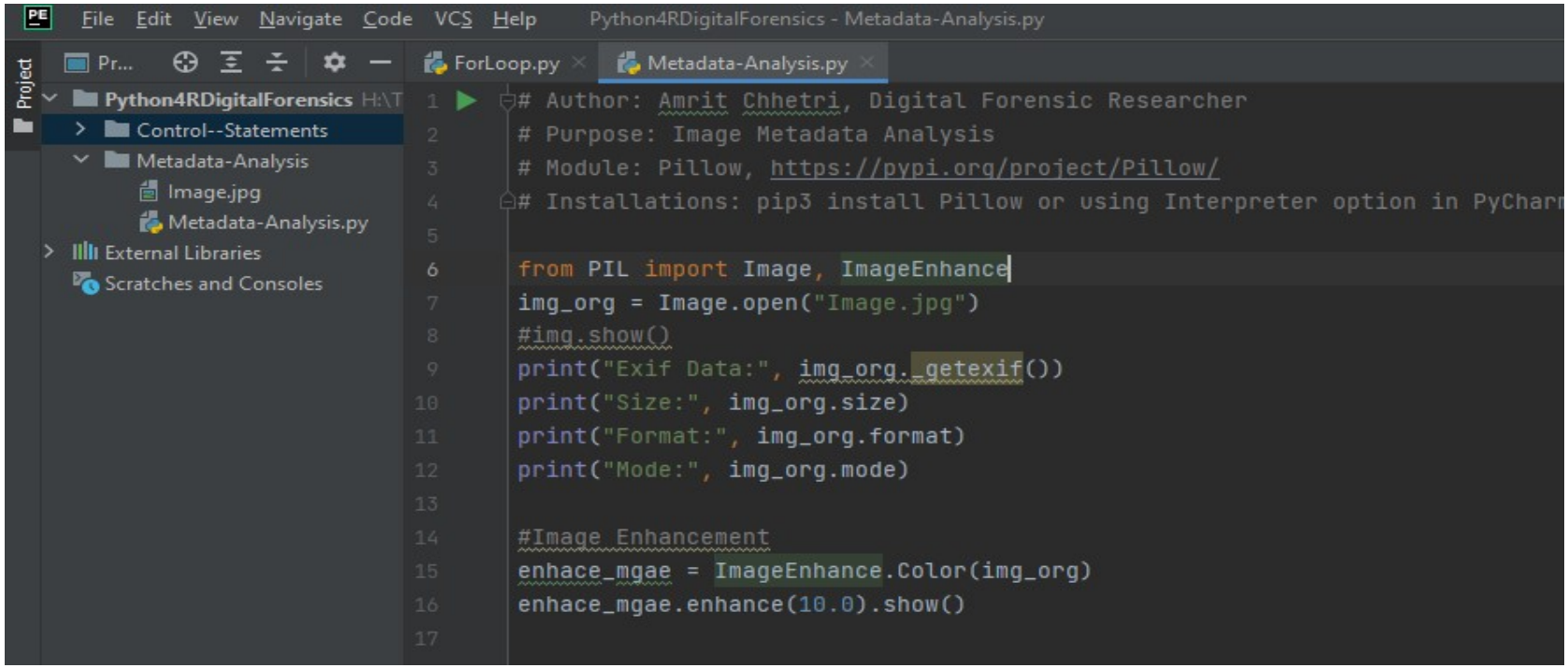
Metadata Analysis using ExifTool(VM):

- **Acquisition of Digital Forensics Evidences or Accessing to Multimedias for Security Testing:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **OSINT Testing Frameworks**
  - **Tools: exiftool on Tracelabs VM(OSINT VM)**
  - **Commands/Tools: $exiftool <filename>**
- **Codes Snippets : (Link to Codes)**



Metadata Analysis using Python Forensics(OSINT):

- **Metadata Analysis of Multimedia Contents:**
  - **Governing Legal Frameworks : Indian Evidence Act 1872, IT Act 2000**
  - **Global Standards: SWDGE's Digital and Multimedia Evidence, https://www.swgde.org/documents/published-by-committee/forensics**
  - **Module: Pillow, https://pypi.org/project/Pillow/**
  - **Installations: pip3 install Pillow or using Interpreter option in PyCharm**
- **Codes Snippets : (Link to Codes)**



Metadata Analysis is common Forensic Practices to know Data about Data or evidences

Mr. Amrit Chhetri

➢Mr. AMRIT CHHETRI is Cyber Security Analyst, Forensics Researcher and Digital Forensics Mentor. He has presented Workshops to great organizations such as CII, AMITY University, Inofsec Foundation, Chandigarh University and he also serving as Sr. Technical Editor of 4N6, India Leading Forensics Journal. He Teaches ***EC-Council's Certifications***, ***Enterprise and End-User Cyber Security*** and Machine Learning/Quantum Machine Learning Courses in RCS, Siliguri and he member of AMITY Research Group. He served as "Jury Member" to various Online and Offline Events in Cyber Security, Machine Learning and Digital Forensics – ***Cyber Security and Digital Forensics eConference from IASR***, "Technological Innovation" from Salesian College, Siliguri and Digital Forensics CTFs Competition(proposed) and ***State/National Level Cyber Security Challenges/Hackathons***. Amrit Chhetri is also well established Forensics, QML and Cyber Security Technology Reviewer and some of his great Reviews include ***DSCI Annual Information Security Summit 2020(AISS), Machine Learning in Cyber Security Research Papers of ICRITO, 4N6 and 5 more***.

➢Amrit Chhetri is an Active Member of different Cyber Security, Digital Forensics and Machine Learning Forums, Organizations and Groups – including KeyCybr(Nasik), NASSCOM Community(India) and OpenMined(UK). He is known for his expertise in Cyber Security and ***Digital Forensics CTFs*** and ***NextGen CSOC Technology Stacks***.

➢Amrit Chhetri loves spending Quality Time with Intelligent GenX Youngs- Males and Female with Coffee and Country/Jazz Songs - mainly discussing innovations, Trends, Business Scopes and Future of "***Machine Learning***" in Healthcare, Fashion, Cyber Security, Digital Marketing …..! He love even number and lucky to have same in his POI(Proof Of Identity) , which is **XXXX-XXXX-0176**

4. Professional Networking

WhatsApp/Mobile Number:

+91-9800692005, +91-8918583776, +91-7583970232, +91-9775907832

Email Addresses:

amritchhetrib@mycyberhubs.com, amritchhetrib@proton.com, amritchhetrib@gmail.com, amritchhetrib.research@gmail.com

Linkedin

Twitter

Koo

Thank You.