Path for Forensic Examiner Aces

CiNPA
Cincinnati Networking Professionals Association
Security Special Interest Group
SECURITY SIG

Tuan Phan

Cincinnati, Ohio

#Digital Forensics

Introducing: Tuan Phan

Tuan works for a big well-known Financial institute...

As an Assistant Vice President (AVP) of eDiscovery and Forensics Lead and has many years of hands-on technical experience, including EF/DF/DFIR & Data Security and Insider Threat Strategy.

He is a Principal Security Engineer for

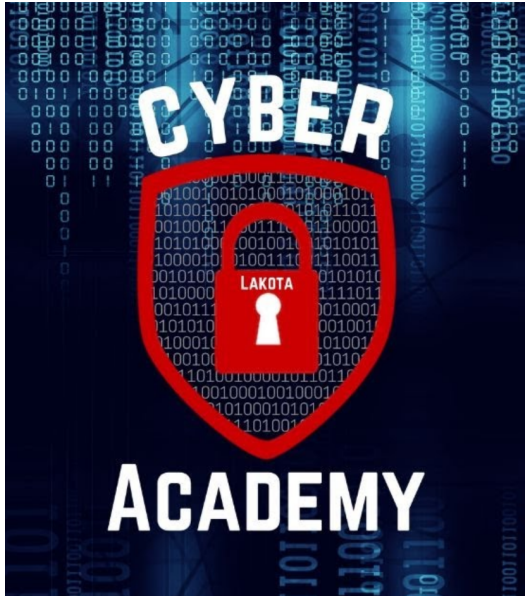
ThreatReel

https://threatreel.com

Follow / contact Tuan:

- https://www.linkedin.com/in/tuanqphan
- https://github.com/phanrensics/slides

Where I Volunteer...



Technical Mentor

WARREN COUNTY CAREER CENTER

Advisory Board Member

Disclaimer!

Yes, the presenter have day jobs. However…

Opinions expressed are based solely on his own independent security research and do not express or reflect the views of his employers.

Agenda

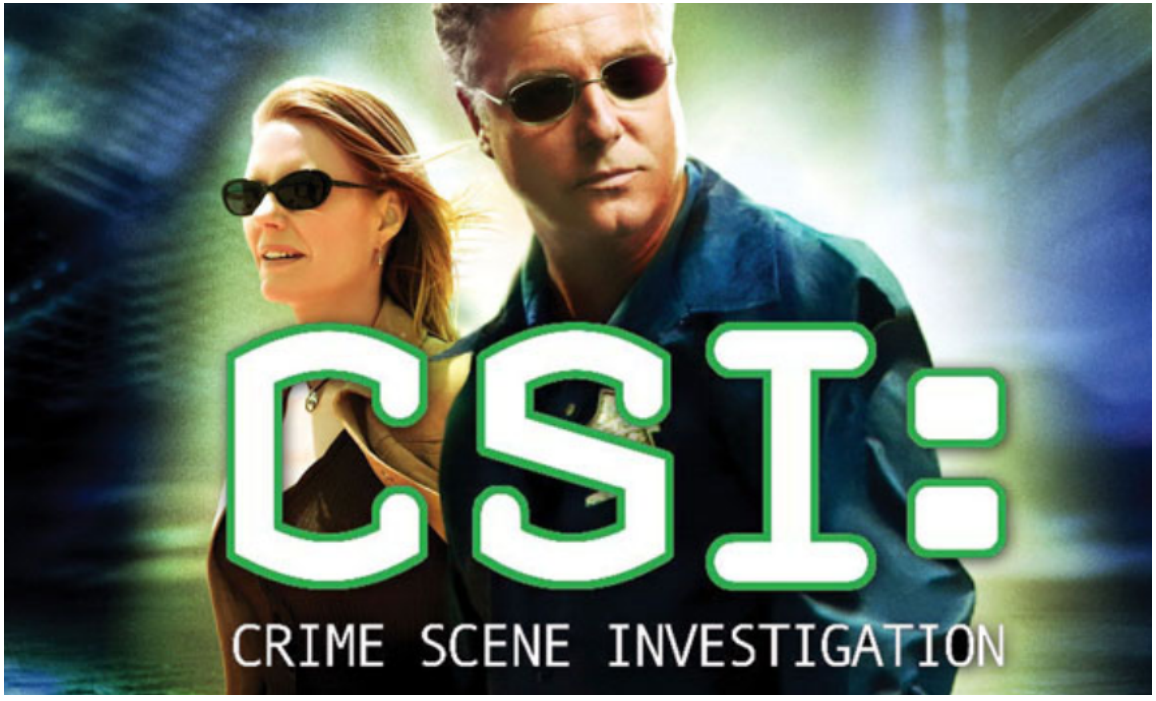
What is a Digital Forensics Examiner (DFE)

- Basic technical skills and the baseline knowledge required for Digital Forensic Examiner.
- Public vs Private
- Experience and skills needed for the job.
- Q&A

Forensic

White Lab Coat

Clean Room


CSI:
CRIME SCENE INVESTIGATION

Buzzwords

- Digital Forensics
  - Cyber Forensics
    - Computer Forensics
      - Digital Cyber
        - Phanrensic

Why This Talk?

- **This talk is inspired by job candidates I participated in interviewing.**
- **Help fill the knowledge, clear the confusion and skill gaps.**
- **Beside SOC/CIRT/AIM/ISIT or others.**
- **Digital Forensics – Is this the career path for you?**

Digital Forensics

- **Collection, Preservation, Analysis, and Reporting**
  - Presented in a Court of Law or other
- **Metadata = Data about data**
  - Author
  - Creation date
  - Modify date
  - Last Access
- **Hash = Fingerprint**

Roles of DF\DFIR

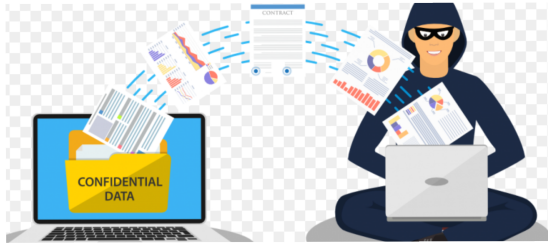
- **Digital Forensics Examiner or Digital Forensics Incident Response (DFIR)**, both investigate security incidents, events, and alerts to answer the classic “Who?”, “What?”, “When?”, “Where?”, “Why?”, and “How?” questions.
- **DF** essentially the collection, **preservation**, and analysis of data.

Aspiring DFE\EF

- Retain a working level knowledge of the following standard Information Security disciplines:
  1) Data collection
  2) Examination
  3) Analysis
  4) Reporting
  5) ***Documentation**

When Digital Forensic Starts

Tied to some kind of criminal or cyber crime investigation.



- Internal investigations for insider threats
- Any events that happen in your company's perimeter.
  - Data being tampered.
  - Intellectual property thief.
  - Someone getting access to something that they shouldn't have had or in a malicious way.
  - Mouse jiggler

Public vs Private

Public Sector

- Work with regional government bureaus
- Deal most with smartphones, tablets, and other devices for evidence of criminal activities such as hacking, fraud, or identity theft, and others.
- Goal is to provide evidence of crime.
- No Legal Right Hold (LRH)
  - FRCP Rule 37
- Lab Accreditation for ISO 9001

Private organization

- Performs the same types of mobile device analyses as public, but less intense in volume.
- Email archives, SIEM, EDR, Compliance Portal, DLP, and other solutions are critical in an enterprise environment;
- Legal Right Hold (LRH)
- Goal is to solve the case of the user, prevent potential future threats and LRH preservation.
- NOT lab are Accreditation for ISO 9001

What Does it Takes to be a DFE

1)Ability to be good under pressure.

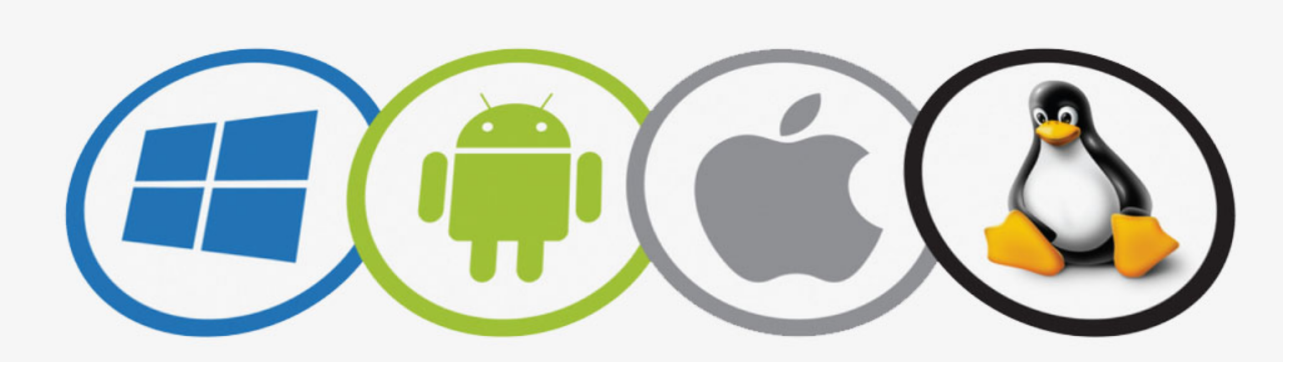
2)May work long hours.

3)Teamwork and willingness to communicate and work well with others.

4)*Testify in court.

OS Basic Skills

- **Understanding various types of OS;**
  - Windows,
  - Linux & Mac
  - IOS
  - Android
  - Others



Artifacts Basic Skills

- **Windows:**
  - Recycle Bin/Deleted data, Registry, Browser artifacts, File Activity, winevt, SRUM, and others.
- **Linux & Mac:**
  - Trash Bin, File System Events, Browser artifacts, File Activity, Recently Used Items, KnowledgeC: Application Focus, Activities & Intents, and others
- **Mobile devices (iOS\Android):**
  - Geo-location, communication, application, media, web browser, and others

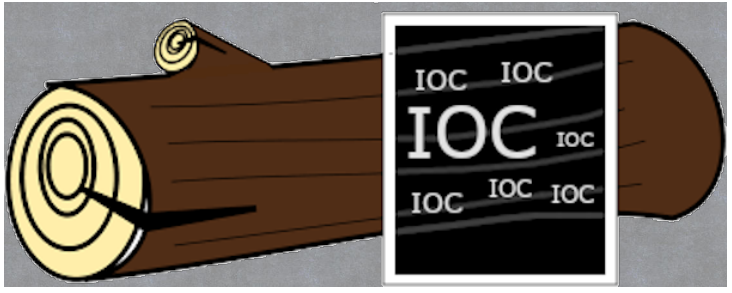
Filesystem Basic Skills

Knowing where things are supposed to be located on an endpoint\devices

Windows • C:\Recycle.bin • \Windows\System32\Config*registry • \Windows\System32\sru\SRUDB.dat • \Users\AppData\Local\ ConnectedDevicesPlatform\<id>\ ActivitiesCache.db	**Linux\Mac** • /home/<USERNAME> • /etc, /var/log, and /etc/passw • *.plist
IOS • /mobile/Library/Safari/ • /mobile/Library/SMS/sms.db • /mobile/Library/CallHistoryDB/	**Android** • /system/packages.list • /system_ce/0/recent_images • /data/system/usagestats/0

*Important Skill: Logs

- The bedrock and starting point of most security investigations begins with any available logs.
- Paramount to becoming a better Digital Forensics.
- Private vs Public



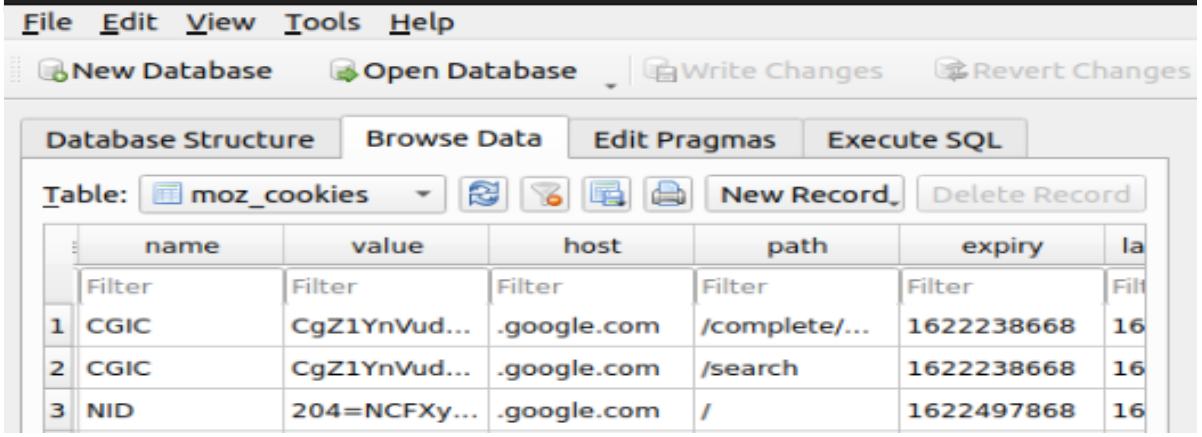
Native Logs

Understanding where logs exist on various endpoints is vitally important

- **Windows Logs**
  - %System32%\winevt\Logs
- **Linux Logs**
  - /var/log/syslog
- **Server Logs**
  - %SystemDrive%\inetpub\logs\LogFiles
- **Application Logs**
  - Depends on applications, some may stored in centralized management

SQL Basics Skills

- **Understand “Structured Query Language” (SQL) to parsed browser history artifacts and other *.DB**

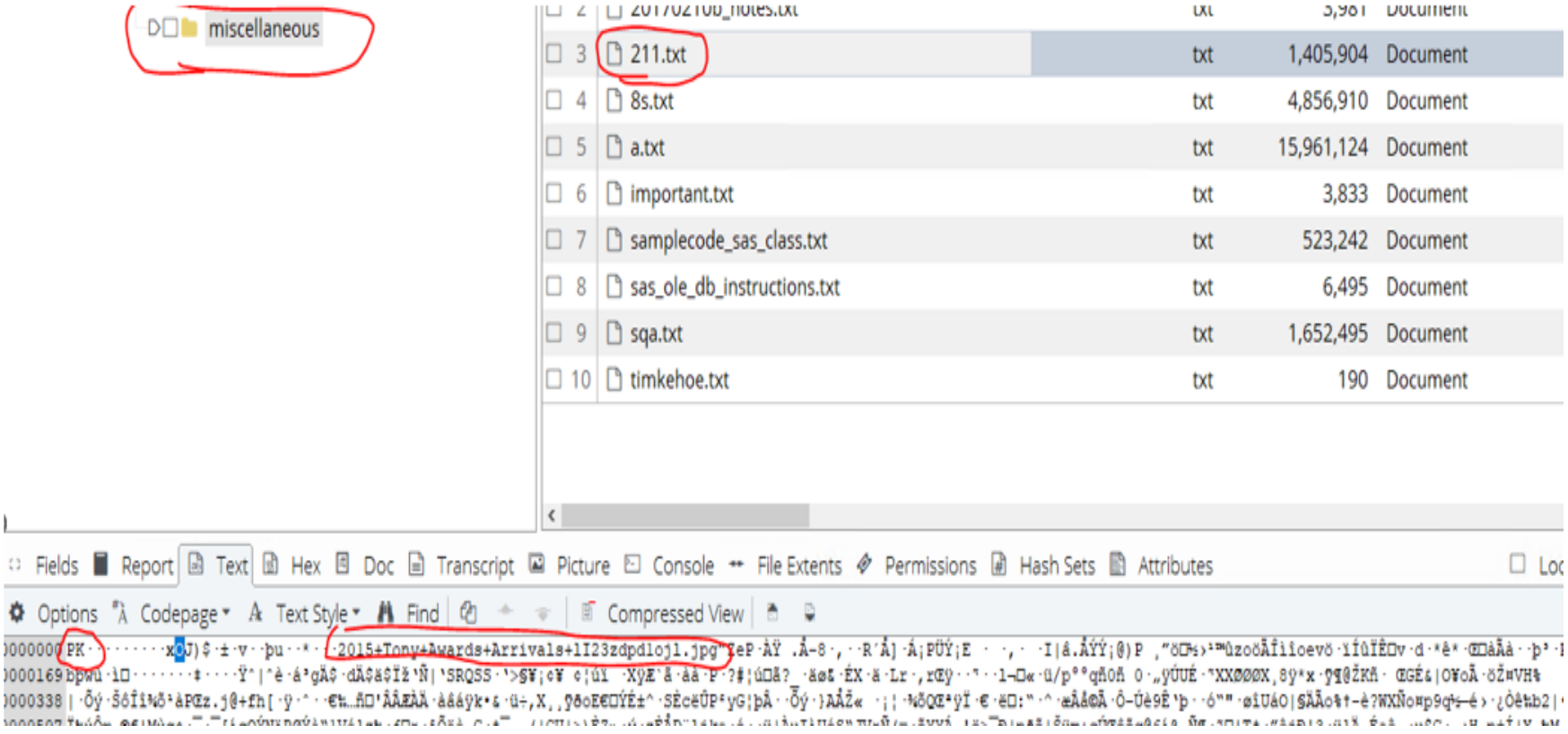


- **Free online training**
  - https://www.sqlcourse.com/beginner-course/
  - https://www.sqlcourse.com/advanced-course/

File Type Identification Skills

- **Understand file signatures, file headers, or whatever you prefer to call them…**
  - Because file extensions can be altered or removed
- **https://www.garykessler.net/library/file_sigs.html**

File Type Example

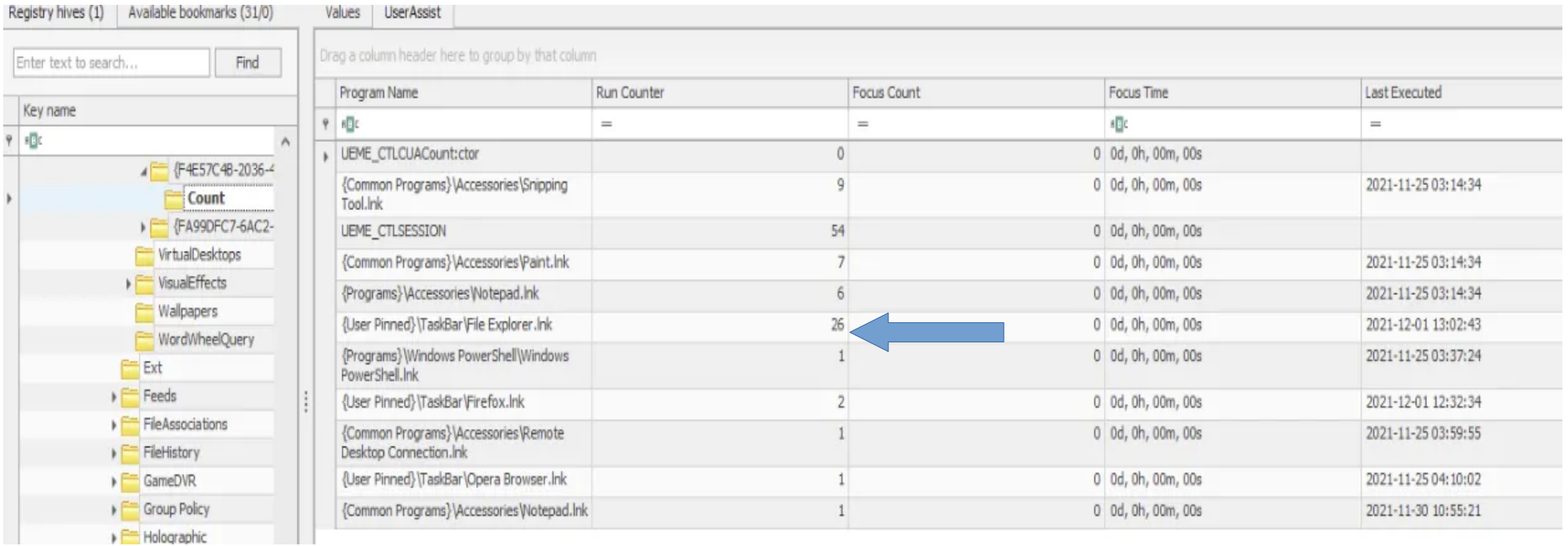


Identify File Execution

- Understand how to know if a file executed on a Windows endpoint
  - Some Examples for the registry key:
    - **UserAssist**
    - **RecentApps**
    - **ShimCache**
    - **CurrentVersion**
    - **Prefetch - %windir%\Prefetch**
    - **etc**

File Execution Sample

- **UserAssist**
  - How many times was the File Explorer launched? (26)

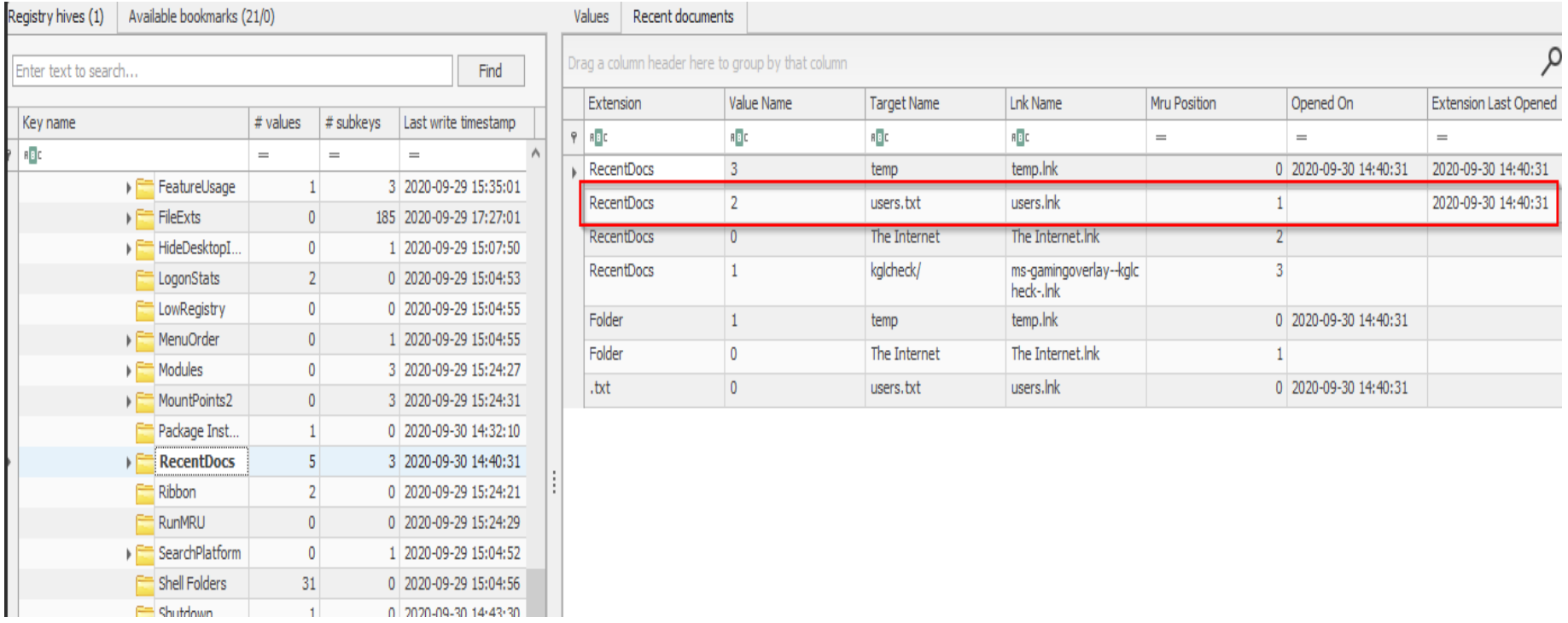


Identify File Activity Skill

- Understand how to know if a file was accessed.
  - This activity is tracked under the following registries below:
    - Jump Lists
    - RecentDocs
    - LastVisitedMRU – last path file opened\executed
    - OpenedSavedPidMRU
    - LNK files
    - ShellBags
    - etc

File Activity Sample

- RecentDocs



Identify USB Activity Skill

- **Understand how to know if a USB was connected.**
  - The majority of USB-related artifacts are located within the Windows Registry
    - SYSTEM\CurrentControlSet\Enum\USBSTOR
    - SYSTEM**MountedDevices**
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer**UserAssist**
  - Windows Event Logs:
    - System event logs may contain entries related to USB device insertions and removals.
    - Event Viewer path: Applications and Services Logs\Microsoft\Windows\DriverFrameworks-UserMode\Operational
  - Windows Prefetch:
    - USB-related executables may be found in C:\Windows\Prefetch\

USB Activity Sample

- **USBSTOR:**
  - SYSTEM\CurrentControlSet\Enum\USBSTOR

- **Things to Record:**
  - Device S/N:
  - Vendor:
  - Product:
  - Service:
  - Container Id:

Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive	00-00-00-00
Capabilities	RegDword	16	
Address	RegDword	2	
HardwareID	RegMultiSz	USBSTOR\Disk_USB_____SanDisk_3.2Gen11.00 ...	00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk	
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	00-00-00-00-00-00
Service	RegSz	disk	00-00
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk d...	00-00-00-00-00-00
FriendlyName	RegSz	USB SanDisk 3.2Gen1 USB Device	00-00
ConfigFlags	RegDword	0	
ContainerID	RegSz	{3deb34e4-837d-5c67-b987-c26b48b8df68}	69-00-63-00-65-00

Understand Order of Volatile

- **Collect and Protect information relating to an incident**
  - Many different data source and protection mechanisms
- **RFC 3227 – Guidelines for Evidence Collection and Archiving**
  - A good set of best practices
- **How Long Does data stick around?**
  - Some media is much more volatile than others
  - Gather data in order from most to less
    - registers, cache
    - routing table, arp cache, process table, kernel statistics, memory
    - temporary file systems
    - disk
    - remote logging and monitoring data that is relevant to the system in question
    - physical configuration, network topology
    - archival media

Steps of Digital Forensics

1)Identification

2)Preservation

3)Analysis & Examination

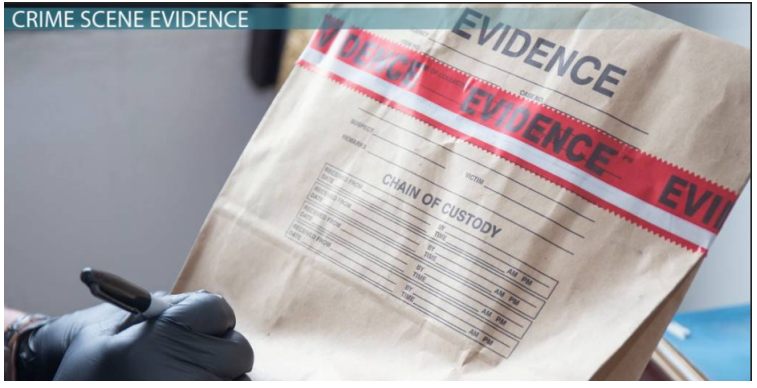
4)Documentation

5)Presentation

Identification

1st step in the forensic process:

- What evidence/source is present
  - Personal computers
  - Mobile devices
  - Shared Networks & Clouds
- Where and how is it stored
- Chain of custody
  - Trail of documentation that links each piece of evidence.
  - Inadmissible in court if items are handled incorrectly.
  - Integrity of the evidence

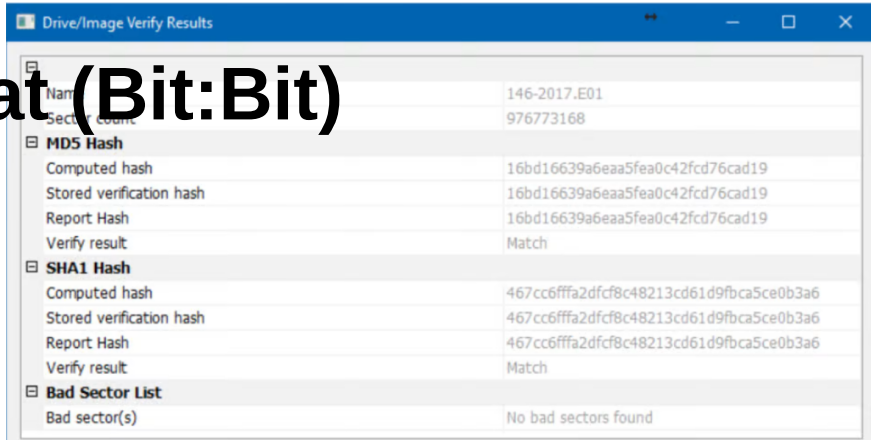


Key parameters in identification:

- Type of information & format

Preservation

- **Extremely important**
  - No matter public or private
  - May be discarded in court
- **Isolate, secure and preserve the state of physical and digital evidence.**
  - Volatile Data, live system Imaging, Forensic Imaging
- **Preserved in the original format (Bit:Bit)**
  - Ensure Image integrity
  - Kept safe and no corruption of the data.

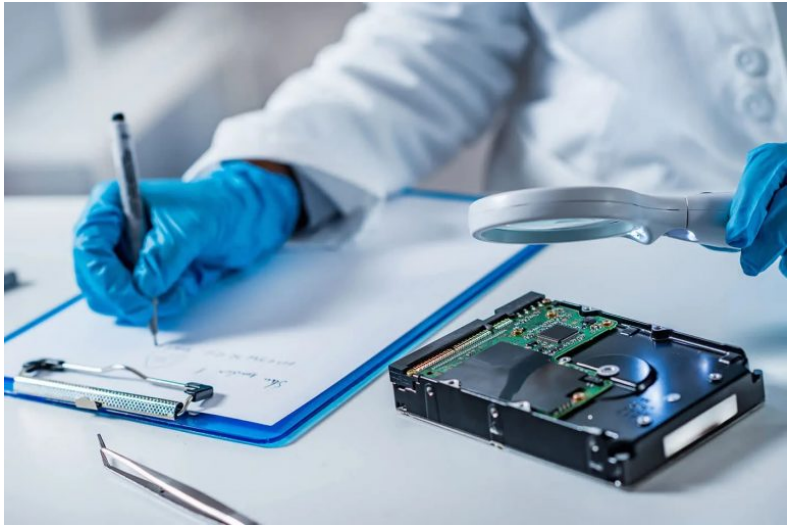


Analysis & Examination

- **Determine significance, reconstruct fragments of data and draw conclusions based on evidence found.**
  - Keywords & filter
- **It may take several iterations of examination and analysis to support a case theory.**
  - Answer the classic “Who?”, “What?”, “When?”, “Where?”, “Why?”, and “How?” questions.

Documentation

- **A record of all visible data must be created.**
  - **Which helps in recreating the scene and reviewing it anytime.**
  - **Involves proper documentation of the case scene along with photograph and others.**
- **A record of all scope of works been done must be created.**
  - **Help regenerating same result no matter who.**
  - **Evidence and data integrity**



Presentation

- **Summarize and provide explanation of the findings \conclusion.**
  - Knows your audience.
  - This should be written in a layperson’s term using abstracted terminologies and reference the specific details.
  - Keep sentences and paragraphs short
  - Quickly get to the point

Forensics Tools for skill building

- **Many tools can be used to perform data analysis on different Operating Systems.**

- **Forensic toolkit for Linux**
  - Kali, Helix, DEFT, Autopsy Sleuth-kit, SIFT

- **Forensic toolkit for Windows**
  - Autopsy, SIFT, FTK imager, Nirsoft

- **Mobile Forensics**
  - SAFT, Autopsy, Belkasoft

Ways to build Forensic skills

- **Follow Cyber Security Linkedin group free training and webnairs.**
  - CYBER SECURITY FORUM INITIATIVE – CSFI
  - Forensic Focus
- **Follow and watch YouTube Digital Forensics Channel**
- **Check out ENISA**

Certifications

- **Some well-known forensic certifications include the following:**
  - CISSP – Certified Information Systems Security Professional
  - CCE – Certified Computer Examiner
  - CFCE – Certified Forensic Computer Examiner
  - GIAC – Certified Forensic Analyst (GCFA)
  - CompTIA A+, Network+, Security+

Salary & Benefits

- **The starting salary for a computer forensics professional depends on various factors.**
  - Whether you're employed in the public or private sector.
  - Degree (s) vs Certification (s)
  - # of years of experience
  - Location

Questions

Who?

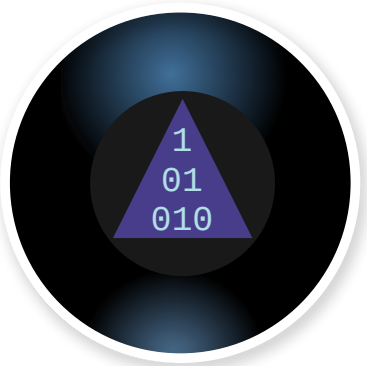
What?

When?

Where?

Why?

How?



Thank you for attending!

Tuan Phan

December 2024

CiNPA

Cincinnati Networking Professionals Association

Security Special Interest Group

SECURITY SIG