Social Media Forensics: Uncovering the Digital Footprint

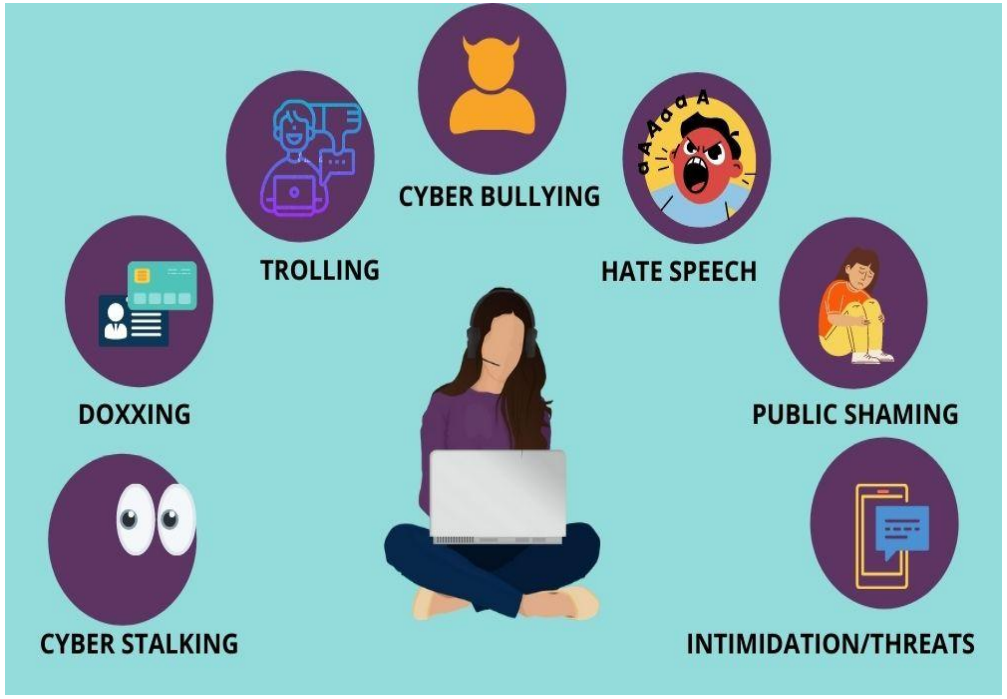
Social Media

- Generally, the term social media is used to refer all the communication channels used for community-based interaction, collaboration, and content- sharing
- Social media use has significantly increased in recent years, aprox. 4 billion in 2024
- It means they are actively engaged in sharing their everyday activities on social media sites
- Cybercriminals to utilize these services for malicious purposes
- Social media is being extensively used to facilitate malicious tasks
- **Social media evidence is a new frontier in digital forensics**
- ***The data found on these websites and applications can imply intent when used in a criminal case***

Social Media Crimes and LEA

- Offenders are engaged in illicit practices such as fraud, cyber stalking, cyber bullying etc.

- Terrorists exploit social media to reach audiences for potential recruits, disseminate messages and organize strategic operations
- Law enforcement agencies (LEAs) take advantage of these information sources for the sake of security
- Social media can be used as a means of surveillance



- **By using digital forensics tools and techniques to review the information captured on social media, inferences can be made about a subject or an event**
- LEAs are also interested in answering the so called six W's: Who, What, When, Where, Why and How
- ***These questions are fundamental and are traditionally raised during criminal investigations***

Social Media Forensic

- **What is Social Media Forensics**
- *Social media forensics is the process of retrieving and analyzing digital evidence from social media platforms to support investigations in criminal or civil cases. The objective is to uncover relevant data, such as posts, photos, messages, and metadata, to help solve legal disputes or criminal cases.*
- **What are the key challenges in Social Media Forensics**
- *The challenges include handling data that may be deleted, encrypted, or spread across multiple platforms, privacy issues related to user consent, and the need for specialized expertise in analyzing non-traditional digital data formats.*

Social Media Forensic - OSINT

- **Open Source Intelligence (OSINT)** *can be incredibly valuable during investigations into social media crimes, as it involves collecting and analyzing publicly available data to gather intelligence, identify patterns, and support criminal investigations.*
  - **Identifying Criminal Activity** (Track hashtags, keywords, and geo-locations related to specific crimes or criminal groups)
  - **Mapping Networks and Connections** (Mapping out digital "social graphs," revealing how people are connected and if they are part of larger networks or coordinated criminal activity
  - **Gathering Evidence of Criminal Activities** (Gather online conversations or posts that support or contradict claims made by individuals or organizations)
  - **Uncovering Anonymous or Fake Accounts** (analyzing user behavior, account activity, and connections, investigators can trace fake accounts back to real individuals or groups.)

Social Media Forensic - SM Platforms

- Social media platforms can provide investigators with **user account** information, such as registration details (e.g., name, IP address, phone number, email), posts, private messages, location data, and device information. This can help trace a suspect or gather evidence for a criminal investigation. They may also supply login history and account activity logs.
- Transparency centers also offer insights into policies, reports on content removal, and other measures taken by the platforms to combat illegal activities and protect users
  - **Facebook** (Meta) Transparency Center: https://transparency.fb.com/
  - **Twitter** Transparency Center: https://transparency.twitter.com/
  - **Google** (YouTube) Transparency Center: https://transparencyreport.google.com/
  - **Instagram** (Meta): https://about.instagram.com/about-us/transparency
  - **TikTok** Transparency Center: https://www.tiktok.com/transparency
- Facebook and Twitter have dedicated law enforcement portals where investigators can submit requests.
  - Requests for user information
  - Content removal
  - Content delistings due to copyright
  - Government requests to remove content
  - Requests to delist content under European privacy law
  - YouTube Community Guidelines enforcement
  - Removals under the Network Enforcement Law

Social Media Forensic Process

- The process of collecting, analyzing, and preserving data from social media platforms to aid in legal or investigative procedures

Collection

- Posts, tweets, status updates, and comments
- Media files (photos, videos)
- Metadata (timestamps, geolocation)

Preservation

- Forensic Images
- Data Time stamping

Analysis

- Keyword search
- Geo-location analysis
- Social network mapping
- Timeline of events
- Connections between individuals or activities

Forensic orchestration

- Packaging
- Securing
- Maintaining

Presentation

- **Releasing evidence to law enforcement**
- **Low Down**
- **Track back report**

Techniques in Social Media Forensic

- **Data Collection Methods**
  - Investigators can use various methods to collect social media data, including direct access through user accounts (with permission), scraping public posts, and using specialized forensic tools to extract data from third-party APIs.
- **Data Preservation**
  - Ensuring the integrity and authenticity of digital evidence is paramount. Preservation methods include creating forensic images, timestamping data, and using write-blockers to prevent alterations during data extraction.
- **Data Analysis**
  - The analysis involves identifying relevant posts, messages, and interactions, examining metadata (such as geolocation and timestamps), and using advanced software tools to detect patterns, verify timelines, or track user movements.

Tools:

- *X1 Social Discovery, Magnet AXIOM, and Belkasoft Evidence Center enable forensic examiners to parse metadata, and search through large datasets to extract useful evidence.*
- *AI-powered tools are increasingly used to identify patterns, anomalies, and relevant content in vast amounts of social media data. These technologies help forensic investigators process and analyze data more efficiently.*

Social Media Tools

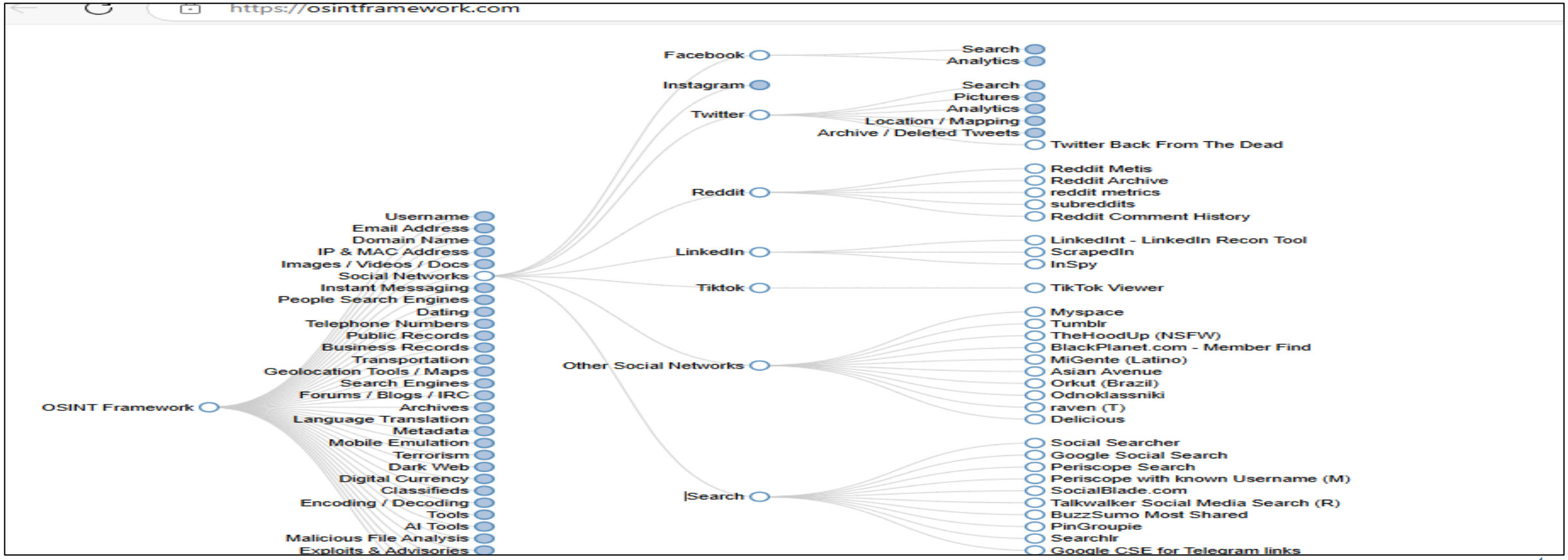
- Social media forensics largely relies on OSINT (Open Source Intelligence) techniques, which focus on gathering publicly available data from various platforms
- While there are several software solutions available, the field is still underdeveloped compared to other forensic domains
- Many tools used for social media forensics are open-source, such as **OSINT Framework**, **Twint**, and **Sherlock**, which allow investigators to gather data from publicly accessible social media accounts and profiles
- However, proprietary tools like **X1 Social Discovery** and **Maltego** offer more advanced features, including data extraction and analysis from private accounts, but they come at a significant cost
- ***Lack of standardized methodologies, privacy concerns, and limitations on accessing certain platform data still pose significant challenges for social media forensics***
- **Consequently, while the number of solutions is growing, the landscape remains limited, with a constant need for innovative tools to bridge the gaps in capabilities**

Social Media Tools

OSINT Framework	A collection of OSINT (Open Source Intelligence) tools for various social media platforms ***https://osintframework.com/***	Open source
Maltego CE	A data mining tool that can be used for social media investigation. ***https://www.maltego.com/***	Propriety but cracks are available
Social-Engineer Toolkit (SET)	Useful for gathering information from social media sites for investigative purposes. ***https://github.com/trustedsec/social-engineer-toolkit***	Open source
Sherlock	A tool to find social media accounts using usernames. ***https://github.com/sherlock-project/sherlock***	Open source
Twint	A Twitter scraping tool that helps in gathering data without the need for API keys. ***https://github.com/twintproject/twint***	Open source
X1 Social Discovery	Perform broad, unified searches across multiple accounts, social media streams and websites from a single interface. ***https://www.x1.com/***	Propriety no crack available

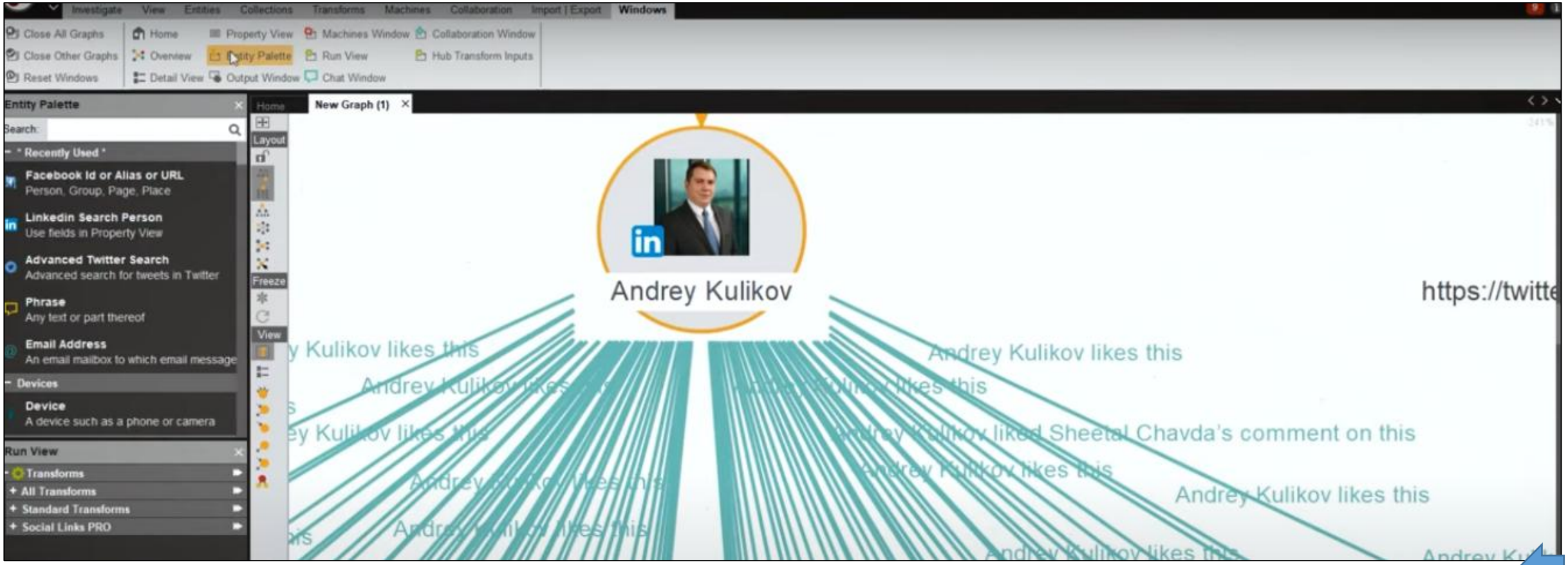
OSINT framework

- OSINT tools within the framework enable effective data harvesting from various online sources, including social media and search engines. They also extend to exploring the Deep and Dark Web, offering insights across multiple sectors.



Maltego

- Maltego is the all-in-one tool for link analysis. Maltego offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable



Social-Engineer Toolkit

- The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly. SET is a product of TrustedSec, LLC – an information security consulting firm located in Cleveland, Ohio.

Sherlock

- Sherlock, an OSINT-powered tool, effortlessly locates social media accounts across multiple platforms like Facebook, Instagram, Twitter, and LinkedIn using a unique username. This Sherlock tool streamlines the OSINT search process, quickly uncovering user profiles and their digital presence.

```
bernard_hackwell@cloudshell:~/cloudshell_open/sherlock$ python3 sherlock --timeout 1 nahamsec
[*] Checking username nahamsec on:
[+] Audiojungle: https://audiojungle.net/user/nahamsec
[+] BitBucket: https://bitbucket.org/nahamsec/
[+] Blogger: https://nahamsec.blogspot.com
[+] Chess: https://www.chess.com/member/nahamsec
[+] Codecademy: https://www.codecademy.com/profiles/nahamsec
[+] Docker Hub: https://hub.docker.com/u/nahamsec/
[+] Dribbble: https://dribbble.com/nahamsec
[+] Facebook: https://www.facebook.com/nahamsec
[+] FortniteTracker: https://fortnitetracker.com/profile/all/nahamsec
[+] GitHub: https://www.github.com/nahamsec
```

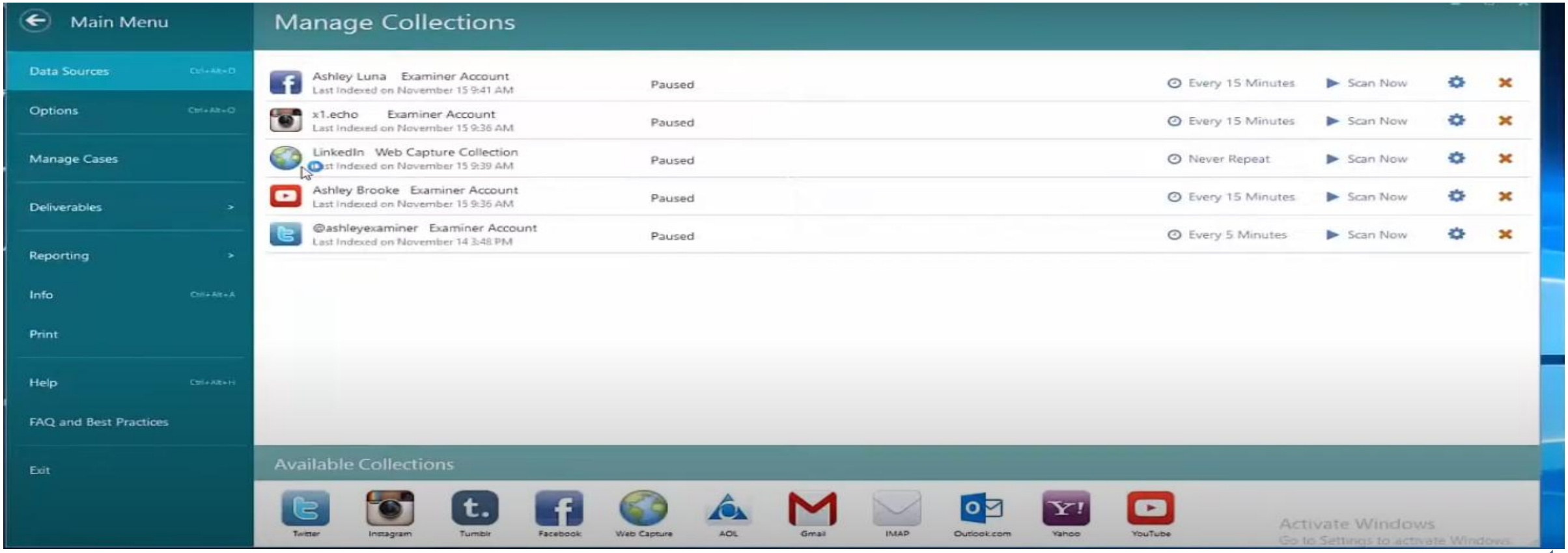
Twint

- Twint utilizes Twitter's search operators to let you scrape Tweets from specific users, scrape Tweets relating to certain topics, hashtags & trends, or sort out sensitive information from Tweets like e-mail and phone numbers. I find this very useful, and you can get really creative with it too.

```
tyto@DESKTOP-3BHGFNH:/mnt/o/androiddevnotes_twint$ twint -u androiddevnotes --since 2020-05-20 --until 2021-03-01 -o twint_androiddevnotes.json --json
1366046060414529541 2021-03-01 00:22:15 +0900 <androiddevnotes> What to look for in a Code Review? ( https://t.co/vcMxg3On5v)  The primary purpose of code r
eview is to make sure that the overall code health of the code base is improving over time.   Engineering Practices to Code Review Open Source Projects and
alike   #AndroidDev #Programming  https://t.co/NZ8pRWKmKL
1366025810038173699 2021-02-28 23:01:47 +0900 <androiddevnotes> The Official Android App for DroidKaigi 2021 ( https://t.co/zX48RlvADU)  Compose processing
&amp; ViewModel processing are performed by Unidirectional data flow.  Tech Stack = Jetpack Compose, Kotlin Coroutines &amp; Flows, Dagger Hilt, Kotlin Mult
iplatform  #AndroidDev #JetpackCompose  https://t.co/OiYuAe8MDb
1365950969259810822 2021-02-28 18:04:23 +0900 <androiddevnotes> Understanding Different Gradle Caches for Android Projects. ( https://t.co/IWYmY213fI)  Part
 1: Gradle's cache of incremental builds, and build cache directory.  Part 2: Android's build cache, Gradle daemon, and dependency caching.  #AndroidDev  ht
tps://t.co/PWArTAP40I
1365627643148734464 2021-02-27 20:39:36 +0900 <androiddevnotes> @amanshuraikwar_ This one is beautiful.
1365625539248091137 2021-02-27 20:31:15 +0900 <androiddevnotes> This is an incredibly massive Codelab. ( https://t.co/jvcg0uIAeP)  Over 10000+ Words, 80000+
 Characters.  It touches lots of concepts of ViewModel, state, events, unidirectional data flow, disheveled design, recomposition, memory in Jetpack Compose
.  #AndroidDev #JetpackCompose
1365588969635737601 2021-02-27 18:05:56 +0900 <androiddevnotes> @codinginflow There's a better chance he may get addicted to incognito mode than enlightenme
nt.
1365003891436228610 2021-02-26 03:21:02 +0900 <androiddevnotes> @codinginflow Yes, you cannot create anonymous anymore. TLDR: gists don't expire anyway.
1365003476049141760 2021-02-26 03:19:23 +0900 <androiddevnotes> @codinginflow Anonymous gists mentioned in the answer is deprecated btw:  https://t.co/PV2Ki
mHpqk
1365002656310194176 2021-02-26 03:16:08 +0900 <androiddevnotes> @codinginflow No.   https://t.co/rno9dKSZwF   https://t.co/3o5RQQvZZq
1364930287306764289 2021-02-25 22:28:34 +0900 <androiddevnotes> Gradle Play Publisher for Android. ( https://t.co/KnsiT0MsnD)  Gradle Play Publisher is Andr
oid's release automation Gradle Plugin.   It can do anything from building, uploading, and then promoting your App Bundle or APK to publishing app listings
and other metadata.  #AndroidDev
1364645120851648519 2021-02-25 03:35:25 +0900 <androiddevnotes> @AndroidDev Rules for entering the Challenge:  https://t.co/JJEuZ40mm2
```

X1 Social Discovery

- X1 Social Discovery™, the industry's first investigative solution specifically designed for eDiscovery and computer forensics professionals to effectively address social media content, website collection, webmail, and YouTube video capture, in one single interface.



Challenges in Social Media Forensics

- **Volatile and Expiring Data**
  - Social media platforms often allow users to delete posts, messages, and accounts. In many cases, data expiration or deletion can hinder an investigation, making it crucial to act quickly and utilize preservation techniques
- **Privacy and Legal Issues**
  - Forensic investigators must navigate privacy concerns and legal restrictions when accessing and using social media data. Legal processes, such as obtaining search warrants, must be followed to ensure the evidence is admissible in court
- **Cross-Platform Data**
  - Social media data is often spread across various platforms (Facebook, Twitter, Instagram, etc.), which can be difficult to track and analyze cohesively. Tools must integrate data from multiple sources to present a comprehensive timeline of events.

The Future of Social Media Forensics

- **Evolving Social Media Platforms**
  - As social media platforms evolve and new platforms emerge, forensic methods must also adapt. This involves keeping pace with changes in platform design, data formats, and privacy regulations
- **Collaboration with AI and Machine Learning**
  - AI and machine learning will continue to play an essential role in enhancing the efficiency and accuracy of social media forensic investigations by identifying patterns and automating tedious tasks
- **Legal and Ethical Implications**
  - As social media forensics becomes more integrated into legal and investigative processes, ethical concerns about privacy, consent, and data usage will continue to grow. Legal frameworks must evolve to protect both users and investigators.

Thank You