EC-Council

CYBER FORENSICS FOR MODERN TECHNOLOGIES: TRACKING CYBERCRIMINALS ACROSS ATTACK VECTORS

EC-Council would like to thank **Lucy Engel**, chief information security officer at BNP Paribas, for authoring this white paper.

Abstract

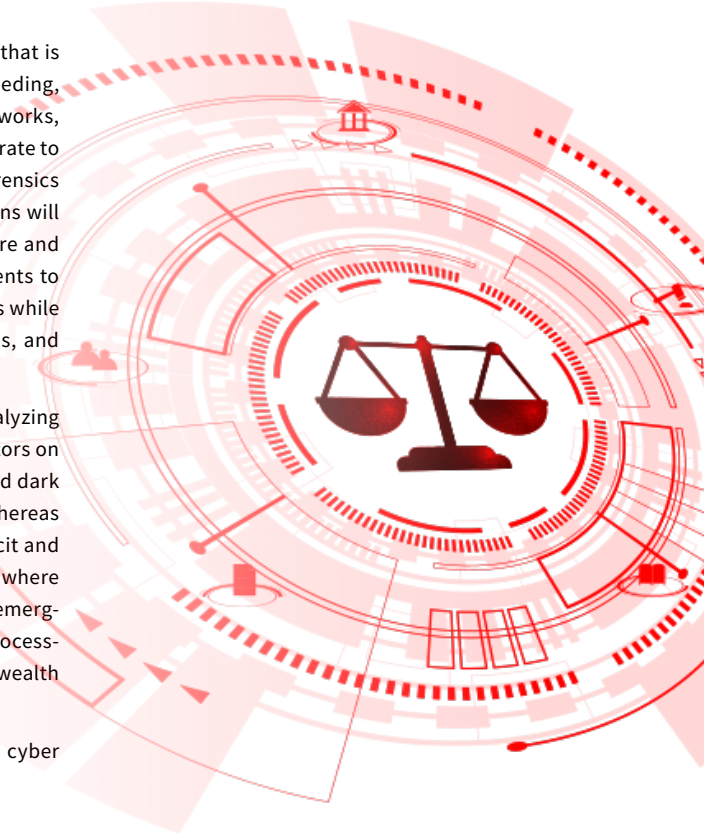
Cyber forensics, also known as digital forensics, is the application of investigative and analytical techniques to obtain digital evidence for use in legal proceedings or other investigations. It is a subset of both cybersecurity and forensic investigation and involves researching, examining, and collecting digital artifacts for further analysis. Cyber forensic methods are typically used to find and preserve digital evidence from networks, storage, and various types of endpoint devices in a forensically sound manner with the aim of presenting it in a court of law. Cyber forensic experts may also participate in private investigations of security incidents, data loss, and corporate espionage. The dark web, cloud, Internet of Things (IoT), databases, and mobile devices are excellent sources of forensic evidence, as malicious actors often rely on these technologies to carry out cyberattacks or conduct reconnaissance. However, they present a complex set of challenges for forensic investigators when it comes to tracking down suspected cybercriminals and threat actors. This paper reviews the approaches taken by digital forensics experts when investigating cybercrime in the context of the dark web, mobile devices, the IoT, and the cloud, among others. It also explores some of the tools and techniques used to trace suspects and monitor them on the dark web.

Keywords: cyber forensics, dark web forensics, IoT forensics, cloud forensics, mobile forensics

Contents

Cyber Forensics for Modern Technologies: Tracking Cybercriminals Across Attack Vectors

Cyber forensics, also commonly referred to as digital forensics, is a discipline at the intersection of cybersecurity and forensic investigation that is defined as the practice of preserving, gathering, and analyzing digital evidence for the purpose of presenting it in a court of law or other proceeding, such as a private investigation or incident report. Cyber forensic techniques can be applied to a broad spectrum of technologies, including networks, mobile devices, emails, databases, and the cloud, among many others. As organizations rapidly complete their digital transformations and migrate to the cloud, digital forensic work is becoming a crucial component of law enforcement, public safety, and national security. Consequently, forensics experts are in higher demand than ever: The U.S. Bureau of Labor Statistics (2022) anticipates that employment of forensic science technicians will grow by 16% between 2020 and 2030—twice the projected rate for all occupations. While most cybersecurity experts focus on building secure and robust digital architectures and defending against various threats, cyber forensic investigators are responsible for examining security incidents to determine their causes and perpetrators. They play an important role in identifying, tracking, and collecting evidence about security incidents while remaining within the bounds of relevant laws and regulations. As such, they typically have domain expertise in criminal law, investigations, and white-collar crime as well as cybersecurity.



By nature, traditional computer forensics is performed using static analysis and deals with data at rest, whereas network forensics involves analyzing information that is dynamic in state (i.e., network traffic). However, the field of cyber forensics today involves not only investigating threat actors on the clear net but also requires delving into the hidden layers of the internet that are not indexed by search engines: the so-called deep web and dark web. The deep web encompasses the vast amount of online data that is not findable via conventional search methods, such as email inboxes, whereas the dark web is a subset of the deep web that is distinguished by the use of anonymizing encryption software and is often the location for illicit and criminal activity (Grannan, n.d.). Extracting information from the deep and dark webs is a particularly complex process for organizations. This is where cyber forensics professionals can step in to help organizations gain insights from digital footprints, open-source intelligence data sources, and emerging darknet threats. Law enforcement agencies and forensics experts use analytics tools driven by artificial intelligence and natural language processing, along with specialized dark web scanning services, for online monitoring and investigative purposes. Social media platforms also contain a wealth of digital information that attackers use to carry out malicious hacks.

This white paper discusses the various online media and technologies through which cybercriminals carry out their attacks, the approaches cyber forensic investigators take to trace them, and common tools used to carry out cyber forensic investigations.

Investigating
Web Application Attacks

Web attacks are typically conducted at the application layer. According to the OWASP Foundation (2021), the top three web application security risks are broken access control, cryptographic failures, and injection, including cross-site scripting (XSS) and SQL injection. Depending on the sophistication of the attack, evidence of the malicious activity may be findable and traceable via browser history files. However, if the attacker is using a virtual machine to obtain automatically assigned IP addresses, the files at the location of network interfaces will not contain useful information. Forensic experts investigating a web application attack can identify post-mortem artifacts on targets' machines and use bash history files to analyze shell activity. The IP address of the attacker's machine and MySQL log files found in back-end databases can be used to identify the attackers' user IDs and entries, including timestamps and other details of attacks.

Organizations today are constantly under attack by cybercriminals, hacktivists, and other external threat actors. Despite advancements in antimalware solutions, these entities

are capable of altering their signatures and are becoming increasingly sophisticated in their attacks, allowing them to breach organizations' network perimeter defenses. Attackers use these "under-the-radar" techniques to bypass enterprises' security mechanisms and breach their networks.

INVESTIGATING WEB APPLICATION ATTACKS USING SPLUNK

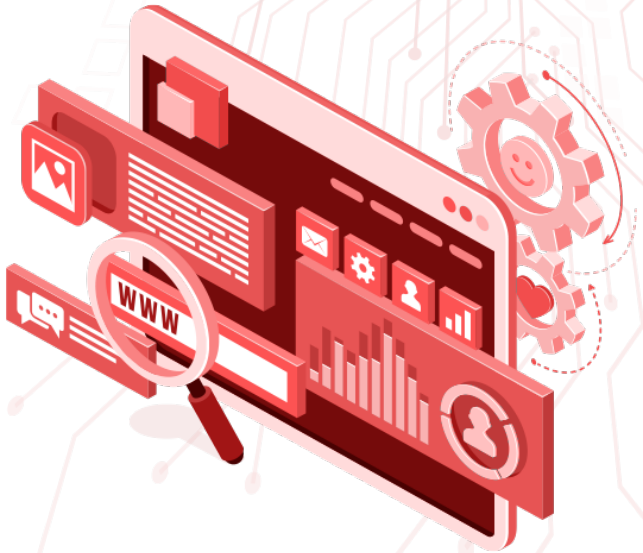
Splunk (n.d.) is a data platform that enables organizations to monitor, alert, analyze, investigate, detect, mitigate, and respond to threats quickly through advanced threat management analytics. Detecting common behavior patterns and network anomalies across cloud and mobile as threats traverse enterprises is a key challenge for organizations today. Splunk User Behavior Analytics (UBA) addresses this by using machine learning algorithms and continuous monitoring to provide context-aware intelligence that lets business owners identify and respond to emerging threats (Casares, 2021). Splunk UBA also detects lateral movements of malware programs across networks. Examples of threats that can be detected using the Splunk UBA tool include:

Investigating Web Application Attacks Using Splunk

Splunk (n.d.) is a data platform that enables organizations to monitor, alert, analyze, investigate, detect, mitigate, and respond to threats quickly through advanced threat management analytics. Detecting common behavior patterns and network anomalies across cloud and mobile as threats traverse enterprises is a key challenge for organizations today. Splunk User Behavior Analytics (UBA) addresses this by using machine learning algorithms and continuous monitoring to provide context-aware intelligence that lets business owners identify and respond to emerging threats (Casares, 2021). Splunk UBA also detects lateral movements of malware programs across networks. Examples of threats that can be detected using the Splunk UBA tool include:

•Account takeovers, in which an attacker escalates the user privileges of an account and attempts to take control of the network

- **Data exfiltration,** which involves stealing sensitive data or confidential information from inside the organization by installing malware
- **Browser exploits,** in which malicious code changes browser security settings and breaches a network (including polymorphic attacks and advanced persistent threats)
- **Anomalous behaviors,** including sudden spikes in network user behaviors, changes in login times and durations, accessing accounts from an unusual location, and taking control over external domains

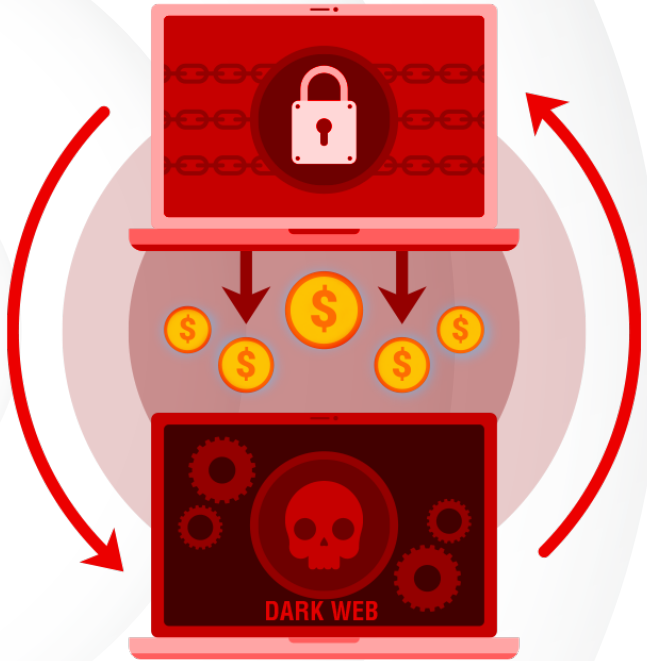


Dark Web Forensics

The dark web is a hidden portion of the deep web where criminals conduct nefarious activities facilitated by the anonymization of their identities and locations. Many cybercriminals launch phishing attacks from the dark web after performing reconnaissance by collecting data from sources like email, social media, and breached companies' databases. Cybercriminals may also gather information from dark web cybercriminal forums and other online channels.

TOR FORENSICS

The best way to conduct dark web forensics is to take a snapshot of a virtual machine (VM) and look for signs of Tor browser activity. Tor is an open-source web browser that anonymizes users by routing encrypted traffic through the relays of the global Tor network (Tor Project, n.d.). Cyber forensic investigators frequently use Tor to browse sites of interest and gather intelligence. However, the anonymous nature of Tor makes it difficult to track down attackers, since there is no sign of browsing activity left behind. Memory dump analysis of Tor browser artifacts and Bitcoin wallets can be performed to trace malicious activity in the Tor network. The browser automatically enters registry logs, and exit relay stations are a reference point for extracting them. Industry-recognized forensic tools such as Encase, AXIOM, and Xways forensics can assist investigators in recovering log files that could provide evidence of Tor browser usage or other signs of dark web activity. When a browser logs out of Tor, there is no way to obtain a copy of the browser history. However, the Tor browser stores SQL database files that contain details such as host names, bookmarks, and search history. Cyber forensics experts can analyze these files to identify the most recent date, time, and location information associated with the hacker. If a user inside the organization is suspected of visiting the dark web, network monitoring tools like Splunk can help companies determine when, where, and how the user accessed darknet websites. Splunk uses high-fidelity reporting tools to reduce network noise, send user alerts, prevent threats, and gain greater visibility into critical security intelligence (Alotaibi et al., 2019).



Database Forensics

Database forensics involves conducting digital investigations on database records and associated metadata. Forensic investigators analyze relational databases using live analysis techniques to find the timestamps that show when rows and columns were updated. Transactions conducted by users through databases can be traced, and users' actions are verified through database inspection and testing. Many database forensics software tools are used to manipulate and analyze data. These programs can perform audit logs of files that show the actions performed by forensic investigators during their inspection. The metadata contents of databases can also be analyzed. Forensic database studies follow a set of standards for documenting and encoding information in large database servers like SQL, Oracle, and others.

Forensic Analysis of SQLite Databases

In the mobile forensics context, SQLite databases are used by mobile operating systems and contain information stored by apps on those devices. SQLite databases are coded in the ANSI C programming language and are designed to process large volumes of data and execute operations quickly (Skulkin & Mikhaylov, 2018). With the growth of iOS and mobile apps, these databases are used to process information because of their high portability and adaptive nature. Such databases are stored as files on mobile devices with several tables and rows. Investigators can extract evidence related to browser history from SQLite databases, which contain information about downloads, URLs, keywords, and other details about various activities. File carving is another procedure used by forensics experts to extract and analyze data from hard disks and storage devices and recover files from unallocated spaces. It structures information from raw data, organizes it, and reconstructs lost artifacts in hard drives, which in turn aid in forensics investigations.

There are a variety of ways to perform forensics of SQLite databases. First, the DB Browser for SQLite (2021) tool can be used to perform a live forensic analysis of database files compatible with SQLite by using a visual interface to browse and search data. It is worth noting that investigators do not gain access to the unused pages of databases when using the database analysis tool. Mari DeGrazia (n.d.) is a leading expert in the cyber forensics community who has written many Python scripts and methodologies for analyzing and detecting various indicators of compromise in different environments. These scripts are publicly available for the community and can be used to access the unused pages of information in these databases and extract strings from blocks. Valuable information about a user's conversations, search history, SMS messages, and other details is contained in free lists. A tool used to recover data from SQLite free lists is Belkasoft (n.d.) Evidence Center X, which finds files hidden inside unallocated spaces on systems and mobile devices. Beginning in version 3.7.0, the SQLite (n.d.) engine introduced the Write Ahead Log (WAL), which tracks changes made to databases in separate files without directly writing over databases. WAL files contain key information that is used in forensics analysis. Investigators can extract the information automatically when analyzing the main files of the SQLite database. The SysTools (n.d.) SQL Log Analyzer tool is software used to perform forensic analysis of SQL databases and recover LDF files. The fn_dblog() function is used to retrieve information but does not reveal details about the transaction logs, deleted records, and timing.

Cloud Forensics

Organizations are investing more into their cloud budgets as cloud adoption is expected to grow in the coming years. However, with increasing cloud migration comes an associated rise in cybercrimes related to cloud-stored data, cloud applications, and cloud-connected devices. Cloud forensics refers to the application of digital forensic techniques to investigate data breaches on the cloud and combat illegal activities related to the usage of cloud services. Cloud forensics combines network, hardware, database, and computer forensics and may be part of both internal and external investigations. In principle, cloud forensic investigations may resemble traditional network forensic investigations, as both involve using forensic tools to examine cybercrimes on networks. However, cloud forensics differs in that the environment in which these cyberattacks are launched (and in which investigations must be conducted) is globally distributed, which creates unique challenges. The multijurisdictional nature of cloud forensics arises from the scattering of cloud servers and data centers across countries and states. Thus, companies must work with law enforcement agencies across geographical locations to collect evidence and track criminals. Another significant challenge in cloud forensics is clients' lack of access to log files. Users under investigation may not have complete data if attackers have deleted it or stored it in various machines across different locations.

Cloud forensics has three main dimensions: technical, organizational, and legal. The technical dimension involves live analysis, data collection, and collaboration in finding and gathering evidence in virtualized environments. End-to-end customer data must be collected, and the tools used depend on the cloud deployments and services related to the case. The organizational dimension involves conducting an examination of cloud services by consulting third parties, such as IT professionals. Cloud service providers and clients may hire cloud security experts to assist forensic examiners when investigating crimes in the cloud. Regarding the legal dimension, legal advisers work with cybercrime professionals and forensic investigators to ensure that no laws or regulations are broken during the investigation. Service-level agreements are defined clearly, and privacy policies are adhered to.

Amazon Web Services (AWS) Cloud and Microsoft Azure are two major cloud service providers. Logging and monitoring activities on AWS Cloud helps experts identify possible data breaches. Applying forensic techniques to the AWS CloudWatch console, Amazon Elastic Compute Cloud ("EC2"), and Azure VMs gives greater visibility into AWS and Azure cloud security incidents and enables faster incident response times for malicious threats. CloudWatch logs can be used to search log data and requests sent by users. Services like Amazon Route 53, AWS Lambda, and AWS CloudTrail offer log fields that enable investigators to input search queries and identify operational issues. Forensic investigators can use these tools to extract information about cases and identify the source locations of threats. Amazon EC2 instances use virtual hard drives to store information, known as Amazon Elastic Block Store volumes. Amazon EC2 lets users create snapshots of the VM and clone physical hard drives to perform forensic investigations. Finally, the Magnet AXIOM platform can be configured to acquire information from an Azure VM. Forensic investigators can use storage containers such as Azure files and disks to create a snapshot. These files can be shared over networks to perform more in-depth investigations (Wall, 2019).

Malware Forensics

The term “malware” refers to malicious computer programs that are installed to hijack and steal sensitive information from computing devices and networks. Examples of malware include viruses, ransomware, rootkits, keyloggers, trojans, spyware, scareware, and worms. The Emotet malware, for example, is sent via spam emails and transmits data to command-and-control servers. It encrypts the data it gathers and uses a command-line interface to execute PowerShell scripts (Baker, 2022). Malware forensics is a branch of digital forensics that deals with collecting, analyzing, and examining data about malware programs designed to infect computer systems with the purpose of determining their origin and intent. Malware analysis aids in the detection of potential threats through scanning for suspicious behaviors and URLs.

There are four types of malware forensic analysis: static, dynamic, hybrid, and memory. In static analysis, the investigator examines malware programs without running them. In dynamic analysis, security professionals execute malware code in a sandbox environment where they can examine how the malware acts in networks when it is run. This makes it easy to find out the true nature of threats and enables analysts to reverse engineer them for investigations. Hybrid analysis combines static and dynamic analysis. Investigators can use hybrid analysis to detect malware threats, even when they are hidden, and map out changes in network behaviors. Hybrid analysis is ideal for quickly spotting indicators of compromise on networks and is capable of handling zero-day threats. In memory analysis, forensic investigators scan for malware artifacts in the RAM of a computer in the aftermath of an infection. This enables them to learn more about the behavior of malware programs and their overall evasiveness after they achieve their objectives.

Malware forensic analysis is often conducted to determine points of compromise and type of malware. Specialized tools such as Volatility are used to examine memory captures to find evidence of persistence not found during forensic analysis of computer hard drives. In 2007, the Volatility Foundation (2020) launched the Volatility Framework, an open-source program for RAM analysis and executing virtual dumps, among other uses. Memory forensics can help determine names of suspicious processes, infection dates, and evidence of persistence that investigators need to determine the scope of a malware infection and assist in planning malware remediation and removal.

Investigating
Email Crimes

Email addresses are being used to impersonate officials from organizations and steal confidential information around the world. Cybercriminals often employ spam messages, email bombs (a type of Denial-of-Service attack), and phishing techniques to deceive targets. The best way to use digital forensics techniques in conducting email investigations is to cooperate with email and internet service providers (ISPs) to track down the source of a malicious email and the corresponding IP addresses of suspects. Email forensics also involves investigating cybercrimes and collecting evidence by scanning email messages, attachments, and online messaging routes and locating the IP addresses of senders and recipients. Network devices like firewalls, switches, and IP routers contain a wealth of data that experts can analyze in the evidence-gathering process. Forensics experts can refer to the log files of network devices to trace the source of email messages and track communications. Email headers contain details about senders, receivers, servers, and devices, which experts can use to conduct their investigations. Most ISPs archive email logs and save copies of sent and received emails on their servers. By collaborating with ISPs, forensics experts can access these emails before they are archived and save time extracting information from messages by skipping the decompression process. Investigators can use enterprise-grade email forensics tools to trace emails and assist in their investigations, including AXIOM, Intella, Stellar Email Forensic Software, and MailXaminer. AXIOM, for example, can recover and analyze evidence from multiple file sources, share powerful reporting, and acquire data from cloud services, whereas Intella uses cluster map technology and email threading to process case evidence and review files.

Another strategy used by investigators is baiting, where investigators send an image source tag to cybercriminals and wait for them to open it. Once they do, investigators can find details about the log entry via the suspect's IP address and use it to track them down. In the event a suspect is using a proxy server, the server's IP address appears, but its logs can still be used to analyze and find out the attacker's true location (Sethi, 2022).

Mobile Forensics

Mobile forensics typically involves searching flash memory and examining files. Mobile forensic software often uses a proprietary boot loader to bypass mobile security measures such as PIN codes and gesture recognition. If forensic investigators have direct access to the physical mobile device, they can use the keypad or touch screen to view files. The file system process of extraction involves accessing the mobile device's operating system and retrieving mobile file system configuration, stored data, and potentially deleted files. Mobile forensics investigators need to ensure that evidence is never tampered with or modified when accessing information. Cellebrite is a digital intelligence platform used to perform mobile forensic investigations and track down cybercriminals. Another common mobile forensics software is Mobile Device Investigator, which is designed for iOS and Android devices. It allows forensics experts to preview content on mobile devices and retrieve files by performing logical data acquisition (Singh, 2022).

Rooting is the process of bypassing a phone's controls by using a custom boot loader program that allows users to access file systems. By rooting an Android device, investigators can overcome the default limitations imposed by manufacturers so that they can collect evidence. The Logcat command-line tool for Android enables system messages to be exported as a text file for further forensic analysis.

Internet of Things Forensics

The Internet of Things (IoT) connects billions of devices worldwide (Vailshery, 2022) and involves the distribution of data among devices, applications, and cloud service providers (CSPs). As data sharing has become essential in everyday life, organizations' cyberattack surfaces have expanded. The cloud is a centralized system for transferring data from the internet to various data centers, meaning that organizations relying on the cloud are not using on-site infrastructures for data storage and retrieval. When devices and appliances are connected via the IoT, this connection is typically facilitated by CSPs.

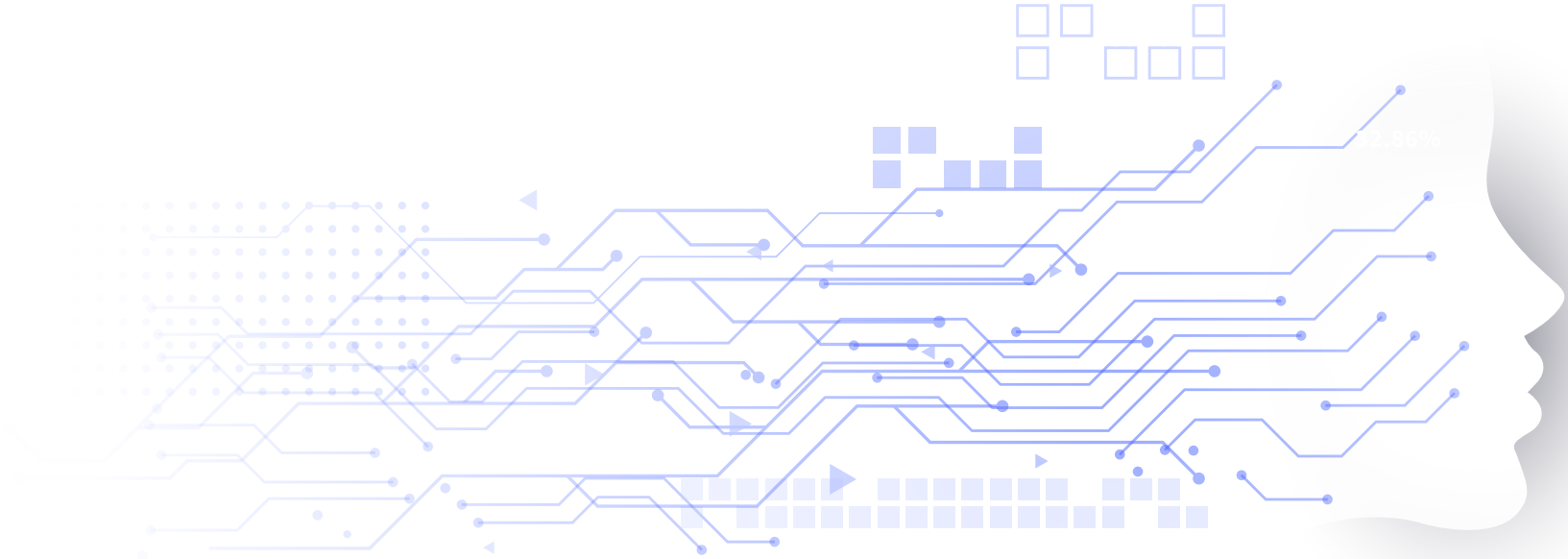
Most smartphones and smart devices do not exhibit forensic readiness when dealing with emerging threats. The IoT is a rapidly growing landscape. Most IoT devices have sensors or actuators that collect data autonomously, making them ideal targets for cybercriminals who are looking to steal vital information. IoT devices generate huge volumes of data and leave digital traces in a number of applications. From storing complete event logs in databases to caching images and thumbnails, including outdoor videos and photographs, IoT devices are a treasure trove of data for both hackers and forensic investigators. Investigators can use the cloud credentials saved by endpoint devices to pinpoint traces of criminal activity on networks, allowing them to track down cybercriminals and obtain evidence for the investigation.

IoT devices have numerous security vulnerabilities that cybercriminals can exploit. Systems like smart home appliances, wearables, televisions, medical devices, and speakers are often easy targets for cybercriminals. A fundamental difference between traditional digital forensics and IoT forensics is the types of devices involved in investigations. For example, large-scale investigations for healthcare systems may involve the analysis of medical implants in addition to more traditional digital systems like desktop computers, mobile devices, and tablets. The source of evidence is another difference between traditional digital and IoT forensics. The IoT has comparatively more terminals from which information can be extracted, including embedded hardware and location tags. Developers have created tools and plugins that investigators can use during IoT forensic analysis to speed up the process. The final step of IoT forensics is examining the physical hardware after initial investigations of software and digital interfaces. It is possible to extract information from several locations over the internet and smartphone applications by simply analyzing the memory of IoT devices. It is estimated that there will be over 29 billion IoT-connected devices worldwide by 2030 (Vailshery, 2022).

IoT forensics presents a complex set of challenges for forensics investigators due to the size of IoT networks, but it also offers unprecedented opportunities to track down perpetrators due to more extensive digital evidence trails. If investigators can collect data from CSPs and extract that data from devices, they can employ a variety of analysis methods. IoT devices may also be used to provide evidence in investigations of nondigital crimes. For example, in a 2015 homicide case in Bentonville, Arkansas, Amazon agreed to release audio recordings from an Amazon Echo device for use as evidence in the investigation, despite initial pushback against investigators' request for a search warrant (Meyers, 2017).

Conclusion

Cyber forensics is rapidly evolving to meet the emerging challenges presented by new technologies and increasingly sophisticated threats. There is a high demand for digital forensics professionals, as law enforcement agencies require additional assistance in analyzing digital information and tracing suspects online. In cases where online data is necessary to provide evidence of criminal activity, cyber forensics can provide concrete proof and assist in reconstructing crime artifacts. Developments in the cyber forensics industry are becoming highly valuable parts of solving criminal investigations, and we anticipate a surge in cyber forensics applications and services within the next few years.



References

Alotaibi, M. A., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Computer forensics:
Dark net forensic framework and tools used for digital evidence detection. *International Journal of Communication Networks and Information Security, 11(3), 424–431.*
http://dx.doi.org/10.17762/ijcnis.v11i3.4407

Baker, K. (2022, January 4). Malware analysis. CrowdStrike.
https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/

Belkasoft. (n.d.). Belkasoft evidence center X. Retrieved July 7, 2022, from
https://belkasoft.com/x

Bureau of Labor Statistics. (2022, April 18). Forensic science technicians. *In Occupational outlook handbook.* U.S. Department of Labor.
https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm

Casares, A. (2021, March 10). Beneath the surface: Monitoring the deep and dark web. *CPO Magazine.*
https://www.cpomagazine.com/cyber-security/beneath-the-surface-monitoring-the-deep-and-dark-web/

DB Browser for SQLite. (2021).
https://sqlitebrowser.org/

DeGrazia, M. (n.d.). *mdegrazia.* GitHub. Retrieved July 7, 2022, from
https://github.com/mdegrazia

Grannan, C. (n.d.). What's the difference between the deep web and the dark web? Britannica.
https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web

Meyers, S. (2017, March 6). Amazon releases audio recordings from Echo device in Bentonville homicide investigation. *KFSM 5NEWS.*
https://www.5newsonline.com/article/news/local/outreach/back-to-school/amazon-releases-audio-recording-from-echo-device-in-bentonville-homicide-investigation/527-ea3b8f24-be80-4c2a-b17a-c023d80ac078

OWASP Foundation. (2021). *OWASP* top ten. https://owasp.org/www-project-top-ten/

Sethi, A. (2022, June 20). Email forensics investigation techniques: A complete guide for security experts. Stellar. https://www.stellarinfo.com/blog/email-forensics-investigation-guide-for-security-experts/

Singh, J. (2022, April 17). Android phone forensic analysis: Unleash hidden evidence. *Data Forensics.* https://www.dataforensics.org/android-phone-forensics-analysis

Skulkin, O., & Mikhaylov, I. (2018, March 14). Forensic analysis of damaged SQLite databases.
Forensic Focus. https://www.forensicfocus.com/articles/forensic-analysis-of-damaged-sqlite-databases/

Splunk. (n.d.). *What is Splunk?* Retrieved July 7, 2022, from
https://www.splunk.com/en_us/about-splunk.html

SQLite. (n.d.). *Write-ahead logging.* Retrieved July 7, 2022, from
https://sqlite.org/wal.html

SysTools. (n.d.). *SysTools SQL log analyzer.* Retrieved July 7, 2022, from https://www.systoolsgroup.com/sql-log-analyzer.html

Tor Project. (n.d.). *Tor project history.* Retrieved July 7, 2022, from
https://www.torproject.org/about/history/

Vailshery, L. S. (2022, June 8). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030.* Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Volatility Foundation. (2020). *About the Volatility Foundation.*
https://www.volatilityfoundation.org/about

Wall, T. (2019, August 20). Forensics in the cloud: What you need to know. *The State of Security.*
https://www.triwire.com/state-of-security/security-data-protection/cloud/forensics-cloud-need-to-know/

EC-Council

www.eccouncil.org