FOR589: **Cybercrime Investigations™**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Adapt traditional investigative methods to the cyber domain and uncover risks specific to your organization
- Investigate dark web marketplaces, forums, and threat actor communications
- Separate actionable leads from background noise to drive informed, evidence-based decisions
- Translate investigative goals into structured collection and case development plans
- Build and manage covert personas to safely access underground communities and collect evidence
- Trace cryptocurrency transactions to uncover threat actors, affiliates, and laundering
- Vet sources and communities for credibility and access to support investigative objectives

Business Takeaways

- Bridge knowledge gaps in cybercrime and crypto crime across your investigative teams
- Strengthen fraud investigations, incident response, and Cyber Threat Intelligence (CTI) capabilities with cybercrime expertise
- Identify and mitigate emerging cybercrime threats by investigating actors before attacks escalate
- Build proactive detection and alerting mechanisms based on criminal behavior
- Investigate initial access, malware deployment, and affiliate partnerships in the underground
- Prioritize investigative leads based on underground trends and threat actor movement
- Apply structured frameworks to track criminal operations from start to finish
- Attribute threat actors with greater confidence through infrastructure and cryptocurrency analysis
- Supplement vendor intel with independent investigative findings tailored to your organization
- Deliver timely, relevant case insights that inform strategic decision-making and response

You Will Receive

- A custom virtual machine preloaded with investigation tools for use during and after class
- Demo access to Authentic8 Silo for safe dark web and surface web investigations
- Demo access to Chainalysis Reactor, enabling hands-on cryptocurrency tracing and blockchain analysis
- Demo access to Maltego, allowing you to visualize relationships between threat actors, infrastructure, and digital footprints using link analysis

Cybercrime investigations are essential for organizations aiming to detect, respond to, and attribute malicious activity, as well as for law enforcement and government agencies working to identify, arrest, and prosecute cybercriminals. FOR589: Cybercrime Investigations™ provides a deep dive into the global cybercrime underground, revealing the tactics and techniques threat actors use to exploit systems and monetize attacks. This course blends investigative tradecraft with modern cybersecurity practices to enhance operations. Whether you're part of a corporate security team, a government investigator, or simply looking to build your skills in tracking and understanding organized cybercrime and threats to your organization, this course will elevate your capabilities.

FOR589: Cybercrime Investigations™ will teach you how to map infrastructure, analyze threat actor capabilities, and identify victims, while working toward attribution of real-world criminal activity. Students will explore criminal underground forums, trace cryptocurrency transactions, and dissect laundering schemes used by cybercriminals. The course emphasizes safe online investigative practices, including creating sock puppets, engaging with threat actors, and infiltrating underground communities. Through hands-on labs and real-world case studies, participants will investigate cyber threats, collect and analyze digital evidence, and uncover the scope, scale, and impact of cybercriminal campaigns—aligning all findings with strategic intelligence priorities.

What is cybercrime investigations and why is it important?

Cybercrime investigations helps organizations anticipate, prevent, and mitigate future cyber threats while aiding law enforcement in investigating and prosecuting cybercriminals. Cybercrime investigations is key to helping organizations to:

- Proactively identify and address looming threats before attacks occur
- Make informed decisions about resource allocation based on real-time threat information
- Support law enforcement with evidence and insights to aid investigations

How will this cybercrime investigations course benefit my career?

The FOR589™ course offers equips you with the skills you need to anticipate, prevent, and mitigate potential cyber threats within your organization. Develop an in-depth understanding of the cybercrime underground while expanding knowledge of traditional intelligence and contemporary cybersecurity. Gain hands-on experience with cybersecurity tools and work on real-life case studies, helping you thwart potential threats before they escalate.

"In the many years I've been doing this, I've taken lots of cybersecurity courses, created them, and taught them. This course is different than any cyber-related course I've ever taken. They showed me things I had not even thought about, and I've been doing this for a long time."

—Jon DiMaggio, Chief Security Strategist, **Analyst1**

Section Descriptions

SECTION 1: Cybercriminal Intelligence

Cybercrime intelligence is the foundation for any successful investigation or threat mitigation strategy. In high-risk environments where attribution errors and OPSEC missteps can have real-world consequences, analysts must apply structured, defensible methodologies. This section introduces the intelligence lifecycle in the context of cybercrime operations—covering requirement setting, collection planning, digital tradecraft, and operational security. Students will learn how to profile threats, manage digital personas, and conduct safe, targeted intelligence collection from underground sources. The goal: turn fragmented data into actionable intelligence to support investigations, disruption efforts, and strategic decisions.

TOPICS: Intelligence Fundamentals & Structured Analysis; Collection Planning & Cybercrime Requirements; Cyberattack Profiling using industry frameworks; Operational Security: Defense-in-Depth Modeling; Persona Development & Sock Puppet Management; Tools for Attribution: Password Pivots, Wallet Analysis, and Forums

SECTION 2: Cryptocurrency Investigations

Cryptocurrencies may appear anonymous, but their pseudonymous nature creates opportunities for exposure. This section trains students to uncover and trace illicit financial activity using blockchain analytics and attribution techniques. From clustering wallets to decoding laundering schemes, students will follow the money through mixers, CoinJoins, peel chains, and more. You'll also examine how cybercriminals cash out, the impact of sanctions, and how off-chain artifacts like KYC records and OSINT enrich attribution. This section equips analysts with investigative tradecraft for mapping threat actor finances, supporting legal action, and recovering stolen assets.

TOPICS: Fundamentals of Blockchain and Cryptocurrency Tracing; UTXO and Account-based Models (Bitcoin, Ethereum); Wallet Clustering, Change Analysis, and Transaction Heuristics; Tracing Obfuscation Methods: Mixers, CoinJoins, Chain Hopping, Peel Chains; Attribution Using OSINT, KYC, Sanctions Data, and Wallet Fingerprinting; Analysis of Laundering Tactics in Real-world Ransomware and Cybercrime Campaigns; Blockchain FININT: Turning Transaction Data into Strategic and Tactical Intelligence

SECTION 3: Cybercrime Underground

The cybercrime underground is a vast, dynamic, and evolving ecosystem of illicit services, marketplaces, and threat actors. In this section, students will learn how to safely navigate and investigate cybercriminal communities across surface, deep, and dark web environments. You'll uncover how forums, leak sites, messaging platforms, and infrastructure tie together into a functional underground economy—and how adversaries interact to buy, sell, and monetize access, data, and capabilities. Students will learn to identify key players, map infrastructure, profile behaviors, and trace victims across ransomware campaigns, infostealer logs, and data leaks. These investigations form the bedrock of effective cybercrime disruption and attribution.

TOPICS: Profiling Forums, Marketplaces, Ransomware Leak Sites, and Messaging Apps; Understanding the Roles of Initial Access Brokers, Ransomware Affiliates, Malware Developers, and Cybercrime Forum Members; Investigating Cybercrime Infrastructure Using Profiling Techniques; Identifying Victims Across Markets, Extortion Sites, and Infostealer Logs; Mapping Capabilities Using Frameworks like MITRE ATT&CK and the Diamond Model; Uncovering Identifiers (Usernames, Passwords, Emails, Wallets) and Behavioral Patterns; Profiling Malware, Phishing, andExploit Services Offered in the Underground; Investigating and Mapping Ransomware Victimology and Campaign Activity; Understanding Adversary Tradecraft, Criminal Ecosystems, and Infrastructure Reuse

SECTION 4: Undercover Operations

Investigating the cybercrime underground requires more than passive observation—it demands placement, access, and trust. In this section, students will learn how to infiltrate gated criminal communities, build credible personas, and collect human intelligence (HUMINT) directly from threat actors. You'll explore both manual and automated approaches to collecting data, from eliciting adversaries through social engineering to scraping dark web content at scale. Students will also learn to assess source credibility, analyze cybercrime infrastructure in Kibana, and map intelligence to countermeasures—equipping them to shift from insight to disruption with precision and confidence.

TOPICS: Persona Creation and Maintaining Access in Cybercriminal Communities; Navigating Underground Forums, Marketplaces, and Encrypted Chats; HUMINT Collection: Spotting, Assessing, Targeting, and Profiling Sources; Social Engineering and Elicitation Tradecraft in Cybercrime Investigations; Automating Dark Web Data Collection Using Scrapers and Evasion Tactics; Visualizing and Analyzing Cybercrime Trends in Kibana; Attribution and Disruption Strategies for Threat Actors and Infrastructure

SECTION 5: Capstone Exercise

The final day of FOR589 is a capstone challenge that focuses on launching an investigation. Students engage in a fun and meaningful exercise that brings together various components of the entire course. The capstone will reinforce the principles taught via a simulated scenario that enables students to practice implementing their newly learned skills. Students will be presented with a simulated investigation involving a fully interactive cybercrime forum. They will have to analyze posts and profiles from the forums, as well as leaked private chat logs and seized databases. There will also be a fictional blockchain ledger that students will use to trace transactions and track threat actors and various types of activities. Students will have to think about how to fulfil intelligence requirements of law enforcement and through a supporting CTI perspective, using the data sets provided that emulate real-world scenarios. Students will be placed in teams and will need to present their findings on what their investigation uncovered, including the steps taken, what they collected, processed, analyzed, and how it can be exploited.

Who Should Attend

- Cyber threat intelligence analysts
- Cyber intelligence professionals
- Criminal actor investigators
- Financial crime investigators
- Threat hunters
- Incident responders
- Forensic analysts
- Information security professionals
- Federal agents and law enforcement professionals
- SANS alumni looking to take their skills to the next level

NICE Framework Work Roles

- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- All-Source Analyst (OPM 111)
- Cyber Crime Investigator (OPM 221)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Forensics Analyst (OPM 212)
- Cyber Defense Incident Responder (OPM 531)
- Cyber Intel Planner (OPM 331)
- Cyber Operator (OPM 331)
- Cyber Ops Planner (OPM 332)
- Cyber Policy and Strategy Planner (OPM 752)
- Data Analyst (OPM 422)
- Exploitation Analyst (OPM 121)
- Law Enforcement/ Counterintelligence Forensics Analyst (OPM 211)
- Mission Assessment Specialist (OPM 112)
- Partner Integration Planner (OPM 333)
- Research & Development Specialist (OPM 661)
- Target Developer (OPM 131)
- Target Network Analyst (OPM 132)
- Threat/Warning Analyst (OPM 141)