SYLLABUS

Course Code	
Course Title	Introduction to Proactive and Reactive Internet Investigation
Course Credit	
Prerequisite	None. Basic computer and Internet navigation skills are recommended.

Course Description

This one-day introductory course equips law enforcement and public safety personnel with foundational knowledge and practical skills for conducting proactive and reactive Internet investigations. Participants will complete a guided group investigation involving a simulated suspicious website and associated digital artifacts and will produce a concise investigative report documenting their observations, findings, evidence, and recommended next steps.

The course introduces proactive and reactive Internet investigation concepts, investigative workflow, preservation and documentation of digital evidence, website and infrastructure investigation, basic log analysis, open-source and threat-intelligence research, and introductory use of investigative and security tools. Guided demonstrations and exercises introduce participants to Nikto, DirBuster, Burp Suite, VirusTotal, and related resources. The course emphasizes investigative reasoning and evidence interpretation rather than advanced cybersecurity exploitation.

Matrix of Outcomes

Institutional Outcome/s	Program Outcomes	Subject Outcome
Apply professional knowledge, critical thinking, ethical conduct, and appropriate investigative methods in addressing public safety and security concerns.	Apply appropriate investigative processes and available technologies in gathering, analyzing, documenting, and communicating information relevant to public safety and law enforcement operations.	Conduct a basic Internet investigation by applying proactive and reactive investigative methods, using appropriate introductory tools and digital artifacts, and documenting evidence-based findings and recommended investigative actions.

Note: Institutional and program outcome wording may be aligned with the official PPSC-prescribed outcomes, if applicable.

Course/Subject Plan

Course/Subject Outcome 1: Conduct a basic Internet investigation by applying proactive and reactive investigative methods, using appropriate introductory tools and digital artifacts, and documenting evidence-based findings and recommended investigative actions.

Content

A. Foundations of Internet Investigation

- Internet investigation in the context of law enforcement and public safety
- Digital footprints and Internet-based evidence
- Proactive vs. reactive Internet investigation
- Investigative questions: Who? What? When? Where? How?
- Indicators, artifacts, leads, evidence, and intelligence
- Attribution limitations and avoiding premature conclusions
- Documentation and preservation of investigative findings
- Ethical, legal, operational, and safety considerations

B. Proactive Internet Investigation

- Identifying suspicious Internet infrastructure and activities
- Investigating domains, websites, IP addresses, URLs, and files
- Website reconnaissance and basic domain, DNS, IP, and hosting information
- Website directories and exposed resources
- Threat-intelligence and reputation sources
- VirusTotal and similar intelligence platforms
- Introduction to Nikto and DirBuster
- Connecting multiple indicators to develop investigative leads

C. Reactive Internet Investigation

- Starting from a reported incident and establishing an initial incident timeline
- Identifying and extracting Indicators of Compromise (IOCs)
- IP addresses, URLs, domains, filenames, hashes, and timestamps
- Basic interpretation of web/server/security logs
- Correlating logs with external intelligence
- Introduction to HTTP requests and responses
- Basic Burp Suite familiarization
- Distinguishing observations from investigative conclusions

D. Guided Internet Investigation Case Study

- Investigation of a fictitious suspicious website within a controlled training environment
- Correlation of website findings, provided logs, selected digital artifacts, and external threat-intelligence information
- Use of web browser/search, VirusTotal, Nikto, DirBuster, Burp Suite, basic IP/domain/DNS resources, and investigation/reporting templates

Time Frame: 8 Training Hours

Activity	Approx. Time
Course orientation and Pre-Assessment	30 min
Foundations of Proactive and Reactive Internet Investigation	2 hrs
Guided Tool Demonstration / Familiarization	1 hr
Group Case Study Briefing	30 min
Guided Group Internet Investigation	2 hrs
Group Reporting / Presentation and Debrief	1 hr
Post-Assessment and Course Synthesis	1 hr
TOTAL	**8 hrs**

Teaching and Learning Experience

1. Establish Prior Knowledge through Pre-Assessment

Participants complete a short individual diagnostic assessment covering Internet investigation concepts, proactive versus reactive investigation, common Internet artifacts, basic indicators of compromise, and familiarity with investigative tools. The instructor uses the results to identify misconceptions and calibrate the depth and pacing of the session.

2. Develop the Investigative Mindset

Participants examine simplified scenarios such as a suspicious website, online scam, malicious download, compromised account, or suspicious IP address. They identify what is known, what is missing, what artifacts may be available, what should be investigated first, and what conclusions cannot yet be made. The instructor distinguishes facts, observations, indicators, intelligence, assumptions, and conclusions.

3. Differentiate Proactive and Reactive Investigation

Participants classify sample activities as proactive, reactive, or potentially both, then construct the workflow: Trigger -> Initial Information -> Evidence/Artifact Collection -> Enrichment -> Correlation -> Findings -> Recommended Action.

4. Guided Investigation of Internet Indicators

Using instructor-provided examples, participants follow the relationship Domain -> IP Address -> Website -> URL -> File -> Hash -> Threat Intelligence -> Related Indicators. They practice documenting source, timestamp, observation, significance, and investigative relevance.

5. Guided Tool Familiarization

The instructor demonstrates Nikto for basic web-server observations, DirBuster for discovering accessible resources, Burp Suite for observing basic HTTP requests and responses, and VirusTotal for researching IP addresses, domains, URLs, and hashes. The emphasis is on what each result tells an investigator, not advanced exploitation.

6. Group Case Investigation

Groups receive a fictitious law-enforcement scenario involving a suspicious website. They are provided an initial complaint/intelligence report, controlled website, selected logs, IP addresses, URLs, filenames/hashes, and guide questions. Groups establish an investigation plan, examine the website and permitted resources, review selected traffic and logs, research indicators, and correlate findings.

7. Evidence Correlation and Investigative Analysis

Groups organize findings into an investigation matrix and explicitly distinguish Confirmed Evidence, Corroborated Finding, Investigative Lead, and Assumption/Unverified Information.

8. Group Presentation and Instructor Feedback

Each group explains what happened, what was investigated, what artifacts were identified, what tools revealed, how artifacts relate, what conclusions are supported, what remains unknown, and what should happen next. The instructor gives feedback on reasoning, interpretation, documentation, and unsupported conclusions.

9. Post-Assessment and Synthesis

Participants complete an individual post-assessment covering the same core competencies measured in the pre-assessment. The instructor synthesizes the investigation framework and discusses how participants can apply it in their respective agencies and when specialist escalation is appropriate.

Assessment

Nature of the Final Product: Group Internet Investigation Report and Case Presentation. Each group submits a concise investigative report documenting its examination of the simulated case and presents its findings to the class.

Task Prompt: Your team has been assigned to conduct an initial Internet investigation involving a suspicious website reported to authorities. Using the information, digital artifacts, logs, controlled investigation environment, and authorized tools provided during the exercise, conduct a preliminary investigation to determine what can reasonably be established from the available information. Document your investigative process, identify and correlate relevant digital artifacts and indicators, distinguish confirmed observations from assumptions, assess the significance of your findings, and recommend appropriate next investigative actions. Your team must be prepared to explain and defend how the available evidence supports your conclusions.

Guide Questions:

1. What information was initially available when the investigation began?
2. What IP addresses, domains, URLs, files, hashes, or other indicators did your group identify?
3. What information did you discover about the suspicious website?
4. What relevant information was identified using Nikto, DirBuster, Burp Suite, VirusTotal, or other provided resources?
5. What significant events or indicators were identified from the provided logs?
6. How are the different artifacts and indicators related to one another?
7. Based strictly on the available evidence, what can your group reasonably conclude about the incident?
8. What additional information, evidence, legal process, technical assistance, or investigative actions would you recommend next?

Criteria/Rubrics:

Criterion	Weight	Description
Investigative Process	20%	Applies a logical and systematic approach to examining the case and available artifacts.
Identification of Relevant Evidence and Indicators	20%	Correctly identifies relevant IPs, URLs, domains, files, hashes, logs, and other artifacts.
Use and Interpretation of Investigative Tools	15%	Appropriately uses introductory tools and correctly interprets their output without overstating results.
Correlation and Analysis	20%	Connects information from multiple sources and develops evidence-supported findings.
Findings and Recommended Actions	15%	Provides reasonable conclusions, identifies limitations, and recommends appropriate next investigative steps.
Documentation and Presentation	10%	Communicates findings clearly, logically, and professionally.
TOTAL	**100%**	

Pre- and Post-Assessment: Approximately 15 items covering proactive vs. reactive investigation, digital artifacts, IP/domain/URL concepts, file hashes, logs, threat intelligence, basic website investigation, interpretation of scanner output, correlation, evidence vs. assumptions, documentation, and appropriate investigative next steps. The pre-assessment is diagnostic and non-graded; the post-assessment measures individual learning.

Learning Resources

- NIST Cybersecurity Framework (CSF) 2.0 and relevant incident response guidance.
- OWASP Web Security Testing Guide and relevant web application security testing resources.
- MITRE ATT&CK knowledge base for understanding adversary behaviors and techniques.
- VirusTotal documentation and threat-intelligence resources.
- PortSwigger Web Security Academy and Burp Suite documentation.
- Nikto Web Scanner documentation.
- DirBuster / OWASP directory enumeration resources.
- Instructor presentation, investigation case scenario, investigation worksheet, controlled Python-based training website, Kali Linux training environment, provided web/server/security logs, pre- and post-assessment forms, group investigation report template, presentation template, and instructor-provided indicators/artifacts.

Course Design Emphasis

Investigate -> Document -> Correlate -> Assess -> Escalate

The course is designed for non-technical, operational law-enforcement and public-safety personnel. Technical tools are used to support investigative reasoning, not to develop advanced penetration-testing

capability. By the end of the course, participants should understand what basic information to collect, how introductory tools and intelligence sources can support an investigation, how to document and correlate findings, what conclusions can and cannot be supported, and when escalation to technical specialists is appropriate.