



Self-Paced Courseware

Reconnaissance and Traceback (Technologies and Tools)

Available at www.podbooks.com.

Laura Chappell, Sr. Protocol/Security Analyst, Protocol Analysis Institute, LLC

Watch narrated and animated moving screen captures as Laura shows you how to investigate a target using local and Internet-based reconnaissance and traceback tools and methods. Use the included reconnaissance and traceback tools to perform lab exercises and obtain information about targets based on their IP address, host/domain name, URL, company/person's name or MAC address.

Course Outline

- Session 1: Overview
- Session 2: Evidence Types
- Session 3: Internet Research
- Session 4: Reconnaissance and Traceback Tools
- Session 5: Traceback by Host/Domain Name or IP Address
- Session 6: Traceback by Email Address
- Session 7: Traceback by Company/Person's Name
- Session 8: Traceback by URL
- Session 9: Traceback by Port Number
- Session 10: Traceback by MAC Address
- Section 11: Hiring Outside Assistance
- Section 12: Resources and References
- Section 13: Lab Exercises and Answers

Course Pricing and Details

This video-based course depicts the step-by-step processes included in the outline above.

Pricing: US \$249.00

Included Materials

This course contains thirteen (13) narrated, audio/video training sessions in AVI and WMV format and a 150+-page Student Guide containing course slides, lab exercise details, and course supplements. Supplements include *Evidence and Reconnaissance Tasks*, *Web Research: Sites to Know*, *Domain Status Codes*, and *Firewall Issues*. The tools and trace files needed to do the lab exercises are contained in the Tools directory and the Trace Files directory.



Duration

19 mins.	Session 1: Overview
13 mins.	Session 2: Evidence Types
41 mins.	Session 3: Internet Research
36 mins.	Session 4: Reconnaissance and Traceback Tools
27 mins.	Session 5: Traceback by Host/Domain Name or IP Address
28 mins.	Session 6: Traceback by Email Address
30 mins.	Session 7: Traceback by Company/Person's Name
18 mins.	Session 8: Traceback by URL
18 mins.	Session 9: Traceback by Port Number
10 mins.	Session 10: Traceback by MAC Address
10 mins.	Section 11: Hiring Outside Assistance
10 mins.	Section 12: Resources and References
54 mins.	Section 13: Lab Exercises and Answers

Detailed Course Outline

Section 1: Overview introduces the course content and format. If you are like me, you'll skip this section and get right into the meat of the course. This section does give you the details on the course elements and Student Guide contents, however.

Section 2: Evidence Types covers where we gather the initial evidence from – email headers, traffic analyzers, log files, honeypots/IDS logs, websites, etc.

Section 3: Internet Research delves into the search engines and search methods for data mining a target on the Internet. If you use Google now – check out the advanced search options listed in this section. One exercise in this section requires you to go back in time and identify the email address of a hacker who held a web site “hostage”.

Section 4: Reconnaissance and Traceback Tools provides a quick overview of both NetScanTools Pro and Sam Spade (Internet-based and client-based versions) and compares the capabilities of each.

Section 5: Traceback by Host/Domain Name or IP Address focuses on using NetScanTools Pro and Sam Spade (where appropriate) to identify the owner of a domain name, the country location and available services on a target and more. You'll see me do a traceback on a host that hit one of my honeypots with an attempted SQL connection. The exercises in this section focus on gathering all the information possible about a domain name and its owner.

Section 6: Traceback by Email Address interprets the header structure of emails as they get forwarded through SMTP servers. You'll watch the traceback process on a questionable email header and learn how to reveal the contents of obscured URLs. Finally, in the section lab exercise you will get a chance to do traceback on an eBay phishing email.

Section 7: Traceback by Company/Person's Name covers methods of using Internet searches and traceback tools to obtain information about a corporate entity or individual. In this section you will do a reconnaissance on yourself and your company name to find out what others can learn about you and your company.

Section 8: Traceback by URL focuses on examining the history of URL pages and delves into the methods for URL obscuring and deciphering.

Section 9: Traceback by Port Number examines suspect traffic with an unrecognized port number. You learn to use Internet resources to look up the port number and research the application further.

Section 10: Traceback by MAC Addresses focuses on the methods to obtain a MAC address from local systems as well as remote systems (on the other side of a routing process).

Section 11: Hiring Outside Assistance compares in-house traceback and reconnaissance to the option of hiring a qualified outside investigator to perform the reconnaissance on your evidence.

Section 12: Resources and References examines the course supplements and key sites to know when doing reconnaissance. In addition, you learn how to get more assistance on running the tools listed in this course.

Section 13: Lab Exercises and Answers provides the instructions for each lab in this course and then shows you the answers as I work the tools and meander the Internet during my research. The lab exercises are contained in this document – refer to the Table of Contents to view the list or jump to a specific lab exercise.

Supplements can be found at the back of this Student Guide and include *Evidence and Reconnaissance Tasks*, *Web Research: Sites to Know*, *Domain Status Codes*, and *Firewall Issues*.

Additional Self-Paced Courses Available

Additional training (including the Ethereal course and the Laura Chappell Master Library™) can be found online at www.podbooks.com.

Register to Attend a Hands-On Class with Laura Chappell

Want more analysis and security training? Check out Laura's course and conference calendar at www.packet-level.com/calendar.