

PEARSON IT

CYBERSECURITY CURRICULUM



SECOND EDITION

A PRACTICAL GUIDE TO DIGITAL FORENSICS INVESTIGATIONS

DR. DARREN R. HAYES

FREE SAMPLE CHAPTER
SHARE WITH OTHERS



A Practical Guide to Digital Forensics Investigations

Dr. Darren R. Hayes

PEARSON

221 River St. Hoboken, NJ, 07030, USA

A Practical Guide to Digital Forensics Investigations

Copyright © 2021 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5991-7

ISBN-10: 0-7897-5991-8

Library of Congress Control Number: 2020906041

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief

Mark Taub

Director, ITP Product Management

Brett Bartow

Senior Editor

James Manly

Development Editor

Christopher Alan Cleveland

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Kitty Wilson

Indexer

Ken Jhonson

Proofreader

Betty Pessagno

Technical Editors

Lorne Dannenbaum
Amir Lakhani

Publishing Coordinator

Cindy Teeters

Designer

Chuti Prasertsith

Compositor

codeMantra

Credits

- Figure 1-1 Screenshot of File metadata © Microsoft 2020
- Figure 2-3 Screenshot of View advanced system settings © Microsoft 2020
- Figure 2-4 Screenshot of System Properties dialog box © Microsoft 2020
- Figure 2-5 Screenshot of Performance Options dialog box © Microsoft 2020
- Figure 2-6 Screenshot of Performance Options dialog box with paging file size © Microsoft 2020
- Figure 2-7 Screenshot of The ASCII text display © 1995-2014 BreakPoint Software, Inc.
- Figure 2-8 Screenshot of The file slack © 1995-2014 BreakPoint Software, Inc.
- Figure 2-9 Screenshot of Viewing the BIOS © Microsoft 2020
- Figure 2-10 Screenshot of Adding the drive to the Evidence Tree © Copyright 2020 AccessData
- Figure 2-11 Screenshot of Expand button © Copyright 2020 AccessData
- Figure 2-12 Screenshot of Partition 1 selected © Copyright 2020 AccessData
- Figure 2-13 Screenshot of NTFS highlighted © Copyright 2020 AccessData
- Figure 2-14 Screenshot of Master File Table displayed in the hex editor © Copyright 2020 AccessData
- Figure 2-15 Screenshot of Prefetch Files © Microsoft 2020
- Figure 2-16 Screenshot of Registry Editor © Microsoft 2020
- Figure 2-17 Screenshot of Two of the data types © Microsoft 2020
- Figure 2-18 Screenshot of Using Disk Defragmenter © Microsoft 2020
- Figure 2-19 Screenshot of The Event Viewer © Microsoft 2020
- Figure 2-20 Screenshot of AutoPlay dialog box © Microsoft 2020
- Figure 2-21 Screenshot of The Backup and Restore Center © Microsoft 2020
- Figure 2-22 Screenshot of System Restore © Microsoft 2020
- Figure 2-23 Screenshot of USB drive information © Microsoft 2020
- Figure 2-24 Screenshot of USBDeview © Microsoft 2020
- Figure 2-25 Screenshot of Sticky Note © Microsoft 2020
- Figure 2-26 Screenshot of InPrivate Browsing with Internet Explorer © Microsoft 2020
- Figure 2-27 Screenshot of Pictures Library © Microsoft 2020
- Figure 2-28 Screenshot of Windows 8 Start screen © Microsoft 2020

- Figure 2-29 Screenshot of Windows 8 Desktop © Microsoft 2020
- Figure 2-30 Screenshot of USB connection history in the Registry Editor © Microsoft 2020
- Figure 3-17 Screenshot of Registry Editor © Microsoft 2020
- Figure 4-13 Screenshot of Add Evidence Item selected © Copyright 2020 AccessData
- Figure 4-14 Screenshot of Physical Drive selected © Copyright 2020 AccessData
- Figure 4-15 Screenshot of USB drive selected © Copyright 2020 AccessData
- Figure 4-16 Screenshot of FTK Imager user interface © Copyright 2020 AccessData
- Figure 4-17 Screenshot of FTK Imager user interface showing deleted files © Copyright 2020 AccessData
- Figure 4-18 Screenshot of FTK Imager user interface © Copyright 2020 AccessData
- Figure 5-1 Screenshot of Fake Name Generator website results © 2006-2020 Corban Works, LLC.
- Figure 5-2 Screenshot of GuerrillaMail website © 2006 - 2020 Jamit Software Limited
- Figure 5-3 Screenshot of mail expire website © mailexpire.com
- Figure 5-4 Screenshot of Mailinator website © 2020 Manybrain, LLC.
- Figure 5-5 Screenshot of Bluffmycall.com website © Bluffmycall.com
- Figure 5-6 Screenshot of SpyDialer.com website © 2020 Spy Dialer, Inc.
- Figure 5-7 Screenshot of Megaproxy.com website © 2000-2018 Megaproxy.com, Inc.
- Figure 5-8 Screenshot of OSINT Framework © osintframework.com
- Figure 5-9 Screenshot of Historical view of www.apple.com (on 8/19/04) using the WayBack-Machine © Internet Archive
- Figure 5-10 Screenshot of NETCRAFT statistics on www.pace.edu © 1995 - 2020 Netcraft Ltd
- Figure 5-11 Screenshot of Alexa website © Alexa Internet, Inc. 1996 - 2019
- Figure 5-12 Screenshot of Zaba Search website © 2020 Zabasearch
- Figure 5-13 Screenshot of US SEARCH website © 1998-2020 PeopleConnect, Inc.
- Figure 5-14 Screenshot of Searchbug website © 1995-2020, Searchbug, Inc.
- Figure 5-15 Screenshot of Skipease website © 2020 Skipease.com
- Figure 5-16 Screenshot of Spokeo website © 2006-2020 Spokeo, Inc.
- Figure 5-17 Screenshot of pipl website © pipl.com
- Figure 5-18 Screenshot of HootSuite website ©2020 Hootsuite Inc.

Figure 5-19	Screenshot of Mibbit website ©Mibbit Ltd
Figure 5-20	Screenshot of Binsearch © 2006-2018 BinSearch
Figure 5-21	Screenshot of Google Groups © Google LLC
Figure 5-22	Screenshot of Blog Search Engine © BlogSearchEngine.com
Figure 5-23	Screenshot of FBI YouTube video of Catherine Greig (Bulger's girlfriend) © Federal Bureau of Investigation
Figure 5-24	Screenshot of LinkedIn © 2020 LinkedIn
Figure 5-25	Screenshot of BRB Publications website © © 1996 – 2018 PeopleConnect, Inc.
Figure 8-1	Screenshot of Windows Event Viewer: DHCP © Microsoft 2020
Figure 8-2	Screenshot of Windows Event Viewer: DNS resolution service © Microsoft 2020
Figure 11-1	Courtesy of U.S. Department of Justice
Figure 11-2	Screenshot of Huntington Beach Jane Doe, 1968 © 2020 Facebook
Unnumbered Figure 11-1	© Copyright 2002-2020 Huntington Beach Police Department
Figure 11-3	Screenshot of Prince Edward Island RCMP Facebook profile © 2020 Facebook
Figure 11-5	Annual Report 2007, Copyright © Interpol. All rights reserved.
Figure 11-6	Annual Report 2007, Copyright © Interpol. All rights reserved.
Figure 12-8	Screenshot of IIOReg Info from BlackBag Technologies © 2020 BlackBag Tech- nologies, Inc. All Rights Reserved
Figure 12-9	Screenshot of PMAP Info from BlackBag Technologies © 2020 BlackBag Technol- ogies, Inc. All Rights Reserved
Figure 12-10	Screenshot of Epoch Converter © 2020 Epoch Converter
Figure 12-11	Screenshot of Sample PList © 1997 NeXT Software, Inc.
Figure 12-12	Screenshot of Webpage Previews © 1997 NeXT Software, Inc.
Figure 12-13	Screenshot of Top sites © 1997 NeXT Software, Inc.
Unnumbered Figure 12-4	© 2020 BBC
Unnumbered Figure 10-1	Facebook, Inc.

Cover

“Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study, and understand it can diminish its value.”

CKA /Shutterstock
Kirk, P. L. (1974) in Thornton, J. I. (ed.) Crime Investigation, 2nd ed, John Wiley & Sons, New York, p. 2.

“fully customizable tool allows your on-the-scene agents to run more than 150 commands on a live computer system.” “provides reports in a simple format for later interpretation by experts or as supportive evidence for subsequent investigation and prosecution.”

Computer Online Forensic Evidence Extractor (COFEE), Microsoft Corporation

“There’s no chance that the iPhone is going to get any significant market share.” “We believe in touch.”

Quote by Microsoft CEO Steve Ballmer

§ Managerial competence § Integrity § Quality § Efficiency § Productivity § Meeting organizational expectations § Health and safety § Security § Management information systems § Qualifications § Training § Maintaining employee competency § Staff development § Environment § Communication § Supervision § Fiscal § Conflict of interest § Response to public needs § Professional staffing § Recommendations and references § Legal compliance § Fiscal responsibility § Accountability § Disclosure and discovery § Work quality § Accreditation § Peer certification § Peer organizations § Research § Ethics

The American Society of Crime Laboratory Directors

“fat ass who should stop eating fast food, and is a douche bag.”

Quoted by Donny Tobolski, Mesa Verde High School, in California

“Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security”

Quote taken from The Tor Project

(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. (2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

18 U.S. Code, Section 2703 (f), Required disclosure of customer communications or records

(a) In General - Not Automatically Objectionable. An opinion is not objectionable just because it embraces an ultimate issue. (b) Exception - In a criminal case, an expert witness must not state an opinion about whether the defendant did or did not have a mental state or condition that constitutes an element of the crime charged or of a defense. Those matters are for the trier of fact alone.

Opinion on an Ultimate Issue’, Federal Rules of Evidence, Rule 704.

(B) Witnesses Who Must Provide a Written Report. Unless otherwise stipulated or ordered by the court, this disclosure must be accompanied by a written report - prepared and signed by the witness - if the witness is one retained or specially employed to provide expert testimony in the case or one whose duties as the party's employee regularly involve giving expert testimony. The report must contain: (i) a complete statement of all opinions the witness will express and the basis and reasons for them; (ii) the facts or data considered by the witness in forming them; (iii) any exhibits that will be used to summarize or support them; (iv) the witness's qualifications, including a list of all publications authored in the previous 10 years; (v) a list of all other cases in which, during the previous 4 years, the witness testified as an expert at trial or by deposition; and (vi) a statement of the compensation to be paid for the study and testimony in the case.

Disclosure of Expert Testimony in the Federal Rules of Civil Procedure; Federal Rule 26(2)(B).

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority; to all Cases affecting Ambassadors, other public Ministers and Consuls; to all Cases of admiralty and maritime Jurisdiction; to Controversies to which the United States shall be a Party; to Controversies between two or more States; between a State and Citizens of another State; between Citizens of different States; between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

Article III, section 2 of the U.S. Constitution.

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Sixth Amendment of the U.S. Constitution

It has no declaration of rights.

George Mason, author of the Virginia Declaration of Rights

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

First Amendment of the U.S. Constitution.

"It can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." "materially and substantially disrupt the work and discipline of the school." *Tinker v. Des Moines Independent Community School District* (No. 21), 393 U.S. 503 (1969).

the reach of school authorities is not without limits.... It would be an unseemly and dangerous precedent to allow the state in the guise of school authorities to reach into a child's home and control his/her actions there...we therefore conclude that the district court correctly ruled that the District's response to Justin's expressive conduct violated the First Amendment guarantee of free expression.

United States Court of Appeals for the Third Circuit, February 2010

"jamfest is cancelled due to the douchebags in central office— here is a letter to get an idea of what to write if you want to write something or call her [school superintendent] to piss her off more." "created a foreseeable risk of substantial disruption"

Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008)

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fourth Amendment of the Constitution

"One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."

Katz v. United States, 389 U.S. 347 (1967)

The right of the people to be secure in their persons, houses, papers, and effects,[a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fourth Amendment of the Constitution

We accept the reality that such over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures.

U.S., Plaintiff-Appellant, v. Comprehensive Drug Testing, Inc., Defendant-Appellee. United States Court of Appeals, Ninth Circuit. (26 Aug, 2009).

Those circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of a suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.

United States v. McConney, 728 F.2d 1195, 1199 (9th Cir.)

names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.

United States v. Carey, No. 14- 50222 (9th Cir. 2016).

Controlled substances, evidence of the possession of controlled substances, which may include, but not be limited to, cash or proceeds from the sales of controlled substances, items, substances, and other paraphernalia designed or used in the weighing, cutting, and packaging of controlled substances, firearms, records, and/or receipts, written or electronically stored, income tax records, checking and savings records, records that show or tend to show ownership or control of the premises and other property used to facilitate the distribution and delivery [of] controlled substances.

United States of America, Plaintiff- Appellee, v. Russell Lane WALSER, Defendant-Appellant. No. 01-8019

“When (the) defendant sat down at the networked computer...he knew that the systems administrator could and likely would monitor his activities,” “Indeed, the undercover agents told (Gorshkov) that they wanted to watch in order to see what he was capable of doing.” “the agents had good reason to fear that if they did not copy the data, (the) defendant’s co-conspirators would destroy the evidence or make it unavailable.”

John C. Coughenour of
Seattle, U.S. District Judge

Monitoring the beeper signals did not invade any legitimate expectation of privacy on respondent’s part, and thus there was neither a “search” nor a “seizure” within the contemplation of the Fourth Amendment. The beeper surveillance amounted principally to following an automobile on public streets and highways. A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.

U.S. v. Knotts 460 U.S. 276
(1983)

[t]he undercarriage is part of the car’s exterior, and as such, is not afforded a reasonable expectation of privacy.

United States of America,
Plaintiff- Appellee, v.
Christopher McIVER,
Defendant-Appellant,
Nos. 98- 30145, 98-30146.
Decided: August 06, 1999

is only a semiprivate area.

United States v. Magana,
512 F.2d 1169, 1171 [9th Cir.
1975]

undercarriage of a vehicle, as part of its exterior, is not entitled to a reasonable expectation of privacy

United States of America,
Plaintiff- Appellee, v.
Juan PINEDA- ORENO,
Defendant-Appellant. No.
08-30385. Decided: January
11, 2010

The Court explicitly distinguished between the limited information discovered by use of the beeper—movements during a discrete journey—and more comprehensive or sustained monitoring of the sort at issue in this case.... Most important for the present case, the Court specifically reserved the question whether a warrant would be required in a case involving twenty-four hour surveillance, stating, “if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”

United States of America,
Appellee v. Lawrence
Maynard, Appellant,
Consolidated with 08- 3034

What motivated the Fourth Amendment historically was the disapproval, the outrage, that our Founding Fathers experienced with general warrants that permitted police indiscriminately to investigate just on the basis of suspicion, not probable cause, and to invade every possession that the individual had in search of a crime.

Justice Sonia Sotomayor,
U.S. Supreme Court

With computers around, it’s now so simple to amass an enormous amount of information. How do we deal with this? Just say nothing has changed?”

Justice Samuel Alito,
Associate Justice of the
Supreme Court of the United
States

We decide whether the attachment of a Global Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.

United States v. Jones 615 F. 3d 544.

Technological advances have produced many valuable tools for law enforcement and, as the years go by, the technology available to aid in the detection of criminal conduct will only become more and more sophisticated. Without judicial oversight, the use of these powerful devices presents a significant and, to our minds, unacceptable risk of abuse. Under our State Constitution, in the absence of exigent circumstances, the installation and use of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause.

The People of the State of New York, Respondent, v. Scott C. WEAVER, Appellant. Decided: May 12, 2009.

Johnson did not produce any evidence that demonstrated his intention to guard the undercarriage of his van from inspection or manipulation by others..... Supreme Court precedent has established not only that a vehicle's exterior lacks a reasonable expectation of privacy, but also that one's travel on public roads does not implicate Fourth Amendment protection against searches and seizures.

State v. Johnson 944 N.E.2d 270 (Ohio Ct. App. 2010)

"I think there was an expectation of privacy that the defendant had for his BlackBerry, that there were not sufficient grounds to authorize the deputy to open that BlackBerry up and, therefore, anything that was discovered as a result of that activity would be suppressed...."

People v. Nottoli, 199 Cal. App.4th 531 (Cal. Ct. App. 2011)

"a routine inventory search of an automobile lawfully impounded by police for violations of municipal parking ordinances," "standard police procedures,"

South Dakota v. Opperman (1976) 428 U.S. 364 [96 S.Ct. 3092]

"the deputies were justified in searching the vehicle's passenger compartment and, 'any containers therein,' In sum, it is our conclusion that, after Reid [Nottoli] was arrested for being under the influence, it was reasonable to believe that evidence relevant to that offense might be found in his vehicle. Consequently, the deputies had unqualified authority under Gant to search the passenger compartment of the vehicle and any container found therein, including Reid's cell phone. It is up to the US Supreme Court to impose any greater limits on officers' authority to search incident to arrest.

People v. Nottoli, 199 Cal. App.4th 531 (Cal. Ct. App. 2011) People v. Nottoli, 199 Cal.App.4th 531 (Cal. Ct. App. 2011)

"I am returning Senate Bill 914 without my signature" "courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections."

Jerry Brown, California Gov.

"ample time for the law enforcement officials to secure a warrant in order to make this significant intrusion"

People v Spinelli, 35 NY2d 77, 81

“Tracking a person’s past movements through CSLI partakes of many of the qualities of GPS monitoring considered in Jones. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in Jones: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person’s whereabouts, subject only to the five-year retention policies of most wireless carriers.” “Government did not obtain a warrant supported by probable cause before acquiring Carpenter’s cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show “reasonable grounds” for believing that the records were “relevant and material to an ongoing investigation.” 18 U. S. C. §2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under §2703(d) is not a permissible mechanism for accessing historical cell-site records.”

United States v. Jones, 565 U. S. 400

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Fifth Amendment of the U.S. Constitution

You have the right to remain silent. Anything you say or do can and will be held against you in a court of law. You have the right to speak to an attorney. If you cannot afford an attorney, one will be appointed for you. Do you understand these rights as they have been read to you?

Miranda v. Arizona, 384 U.S. 436 (1966).

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Sixth Amendment of the U.S. Constitution

in all criminal prosecutions, the accused shall enjoy the right...to be confronted with the witnesses against him.

Sixth Amendment of the U.S. Constitution

Section 2511 of Title 18 prohibits the unauthorized interception, disclosure, and use of wire, oral, or electronic communications. The prohibitions are absolute, subject only to the specific exemptions in Title III. Consequently, unless an interception is specifically authorized, it is impermissible and, assuming existence of the requisite criminal intent, in violation of

Federal Wiretap Act (18 U.S. Code § 2511),
Interception and disclosure of wire, oral, or electronic communications prohibited 18 U.S.C. § 2511.

“combat fraud and theft of service.” (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Federal Wiretap Act (18 U.S. Code § 2511 (2)(a)(i)),
Interception and disclosure of wire, oral, or electronic communications prohibited Federal Wiretap Act (18 U.S. Code § 2510(17))

“having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;”

Corporate Espionage (18 U.S. Code § 1030 (a)(1)).
Fraud and related activity in connection with computers

“records of session times and durations,” “any temporarily assigned network address.”

USA PATRIOT Act (18 U.S. Code § 2703 (c)(2)).
Required disclosure of customer communications or records

§ Title I: The “WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998,” implements the WIPO treaties.
§ Title II: The “Online Copyright Infringement Liability Limitation Act” creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.
§ Title III: The “Computer Maintenance Competition Assurance Act” creates an exemption for making a copy of a computer program by activating a computer for purposes of maintenance or repair.
§ Title IV: Contains six miscellaneous provisions, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, “webcasting” of sound recordings on the Internet, and the applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.

President Bill Clinton, The Digital Millennium Copyright Act (DMCA), 1998, www.copyright.gov/legislation/dmca.pdf.

Anonymity is a shield from the tyranny of the majority [that] exemplifies the purpose [of the First Amendment]: ‘to protect unpopular individuals from retaliation...at the hand of an intolerant society.’

McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 357 (1995)

Just when a scientific principal or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs. (emphasis added).

Frye v. United States, 293 F. 1013 (D.C. Cir 1923).

scientific, technical, or other specialized knowledge.

Rule 702, Testimony by Expert Witnesses, Federal Rules of Evidence

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

Rule 702, Testimony by Expert Witnesses, Federal Rules of Evidence

§ (i) A complete statement of all opinions the witness will express and the basis and reasons for them; § (ii) The facts or data considered by the witness in forming them; § (iii) Any exhibits that will be used to summarize or support them; § (iv) The witness's qualifications, including a list of all publications authored in the previous 10 years; § (v) A list of all other cases in which, during the previous 4 years, the witness testified as an expert at trial or by deposition; and § (vi) A statement of the compensation to be paid for the study and testimony in the case.

Rule 26 (2)(B) & (3)(A), Duty to Disclose; General Provisions Governing Discovery, Federal Rules of Civil Procedure

§ (i) The name and, if not previously provided, the address and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises; § (ii) The designation of those witnesses whose testimony the party expects to present by deposition and, if not taken stenographically, a transcript of the pertinent parts of the deposition; and § (iii) An identification of each document or other exhibit, including summaries of other evidence—separately identifying those items the party expects to offer and those it may offer if the need arises.

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

Rule 803, Exceptions to the Rule Against Hearsay, Federal Rules of Evidence

“the by-product of a machine operation which uses for its input ‘statements’ entered into the machine” “was generated solely by the electrical and mechanical operations of the computer and telephone equipment.”

regular practice of that business activity

The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

Facts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passion, they cannot alter the state of facts and evidence.

§ Maintain a Cybersecurity Program § Cybersecurity Policy § Role of the CISO § Pen Testing & Vulnerability Assessment § Audit Trail § Access Privileges § Application Security § Risk Assessment § Qualified Personnel & Intelligence § Third Party Service Provider § Multi-Factor Authentication § Limitations on Data Retention § Training & Monitoring § Encryption of Non-Public Information § Incident Response Plan § Notices to Superintendent

§ Airports, aircraft and airlines; § Banks and authorized foreign banks; § Inter-provincial or international transportation companies; § Telecommunications companies; § Offshore drilling operations; and § Radio and television broadcasters.

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals

“Photographs” includes “still photographs, X-ray films, video tapes, and motion pictures.” An “original” can include a negative or a print from the negative. A “duplicate” is “a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording.” “other output readable by sight”

Secure Enclave is Secure Enclave is a coprocessor fabricated within the system on chip (SoC). It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised.

State v. Armstead, No. 82-KA- 0896, May 23, 1983.

Rule 803, Exceptions to the Rule Against Hearsay, Federal Rules of Evidence

Rule 901, Requirement of Authentication or Identification, Federal Rules of Evidence

John Adams, Second President of the United States (1797-1801).

The New York State (NYS) Department of Financial Services (DFS), Section 500, 2017

Canada Personal Information Protection and Electronic Documents Act (PIPEDA), 2000

Directive 95/46/EC of the European Parliament and of the Council

Article X, Federal Rules of Evidence (FRE), Rule 1001: Contents of Writings, Recordings and Photographs

Product security certifications, validations, and guidance for SEP: Secure Key Store, Apple Inc.

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it. I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at <http://tydgcckykipbu6uz.onion>. Let me know what you think... the best and brightest IT pro in the bitcoin community [to] be the lead developer in a venture-backed bitcoin startup company "anybody know someone that works for UPS, FedEx, or DHL?"

Quoted by Ross William Ulbricht, American convict

How can I connect to a Tor hidden service using curl in php? I'm trying to connect to a tor hidden service using the following php: `$url = 'http://jhiwjllqpyawmpjx.onion/' $ch = curl_init(); curl_setopt($ch, CURLOPT_URL, $url); curl_setopt($ch, CURLOPT_RETURNTRANSFER, true); curl_setopt($ch, CURLOPT_PROXY, "http://127.0.0.1:9050/"); curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5); $output = curl_exec($ch); $curl_error = curl_error($ch); curl_close($ch); print_r($output); print_r($curl_error);` when I run it I get the following error: Couldn't resolve host name However, when I run the following command from my command line in ubuntu: `curl -v --socks5-hostname localhost:9050 http://jhiwjllqpyawmpjx.onion` I get a response as expected the php cURL documentations says this: `--socks5-hostname` Use the specified SOCKS5 proxy (and let the proxy resolve the host name). I believe the reason it works from the command line is because Tor (the proxy) is resolving the .onion hostname, which it recognizes. When running the php above, my guess is that cURL or php is trying to resolve the .onion hostname and doesn't recognize it. I've searched for a way to tell cURL/php to let the proxy resolve the hostname, but can't find a way. There is a very similar question here: cURL request using socks5 proxy fails when using PHP but works through the command line

Quoted by Ross William Ulbricht, American convict, April 2012

Stack Exchange Inc. "How can I connect to a Tor hidden service using cURL in PHP?" <http://stackoverflow.com/questions/15445285>

"(1) obtain subscriber information associated with the Subject Server; (2) collect routing information for communications sent to and from the Subject Server, including historical routing data from the prior 90 days; and (3) covertly image the contents of the Subject Server"

United States of America v. Ross William Ulbricht. S1 14 Cr. 68 (KBF) (S.D.N.Y., 2014).

"failed to submit anything establishing that he has a personal privacy interest in the Icelandic server or any of the other items imaged and/or searched and/or seized"

United States of America v. Ross William Ulbricht. No. 18-691 (2d Cir. Jan. 24, 2019)

I am creating a year of prosperity and power beyond what I have ever experienced. Silk Road is going to become a phenomenon and at least one person will tell me about it, unknowing that I was its creator. I felt compelled to reveal myself to her. It was terrible.

Quoted by Ross William Ulbricht, American convict

I told her I have secrets. She already knows I work with bitcoin wick [sic] is terrible. I'm so stupid. Everyone knows I am working on a bitcoin exchange. I always thought honesty was the best policy and now I don't know what to do. I should have just told everyone I am a freelance programmer or something, but I had to tell half-truths. It felt wrong to lie completely so I tried to tell the truth without revealing the bad parts, but now I am in a jam. Everyone knows too much, dammit.

§ Conspiracy to commit acts of terrorism transcending national boundaries § Conspiracy to commit aircraft piracy § Conspiracy to destroy aircraft § Conspiracy to use weapons of mass destruction § Conspiracy to murder United States employees § Conspiracy to destroy property of the United States

[The] authentication information (such as the MD5 message digest and other accepted computer forensic methods) is critical as without it, it is impossible to verify that the duplicate hard drives are an exact copy of those that exist on the original systems. Likewise, without such information it is impossible to determine if the material retrieved from the hard drives is accurate.

"NIST does not 'approve' any computer forensic tools. Instead, it merely reports the results of its testing. Moreover, Mr. Allison wrongly identifies Linux dd as the 'only one method...approved by [NIST]'" "there would not ordinarily be any MD5 or SH-1 hash values to disclose to the defense for any computer drives imaged with SafeBack or a Logicube disk duplicator."

"any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to annoy, abuse, threaten, or harass another person."

"Jumping off the gw bridge, sorry." "making out with a dude." "Anyone with iChat I dare you to video chat me between the hours of 9:30 and 12. Yes, it's happening again." "Watch out, he may come for you when you're sleeping." "It keeps the gays away."

We disapproved the wholesale seizure of the documents and particularly the government's failure to return the materials that were not the object of the search once they had been segregated. Id. at 596-97. However, we saw no reason to suppress the properly seized materials just because the government had taken more than authorized by the warrant.

"Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials"

United States District Court for the Eastern District of Virginia

United States v. Zacarias Moussaoui, Criminal No. 01-455-A, United States District Court, E.D. Virginia, Jun 18, 2002

United States v. Zacarias Moussaoui, Criminal No. 01-455-A, United States District Court, E.D. Virginia, Jun 18, 2002

U.S. Code Title 47. TELECOMMUNICATIONS. Section 223. Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications

State of New Jersey vs. Dharun Ravi, Supreme Court of New Jersey

United States v. Comprehensive Drug Testing, Inc., United States Court of Appeals, 513 F.3d 1085 (9th Cir. 2008)

State of Arkansas v. James A. Bates, Case No. 2016-370-2 (Ark. Cir.), Feb. 17, 2017

“Starting May 1, the App Store will no longer accept new apps or app updates that access the UDID; please update your apps and servers to associate users with the Vendor or Advertising identifiers introduced in iOS 6”

Using Identifiers in Your Apps, March 21, 2013, © 2020 Apple Inc.

“may also collect the precise location of your device when the app is running in the foreground or background”

Uber Privacy Notice, February 28, 2020, © Uber Technologies Inc

“Uber collects your location (i) when the app is open and (ii) from the time of the trip request through five minutes after the trip ends”

Uber Technologies Inc

“improve pickups, drop-offs, customer service, and to enhance safety”

Uber Technologies Inc

§ Phone number analysis § IMSI number analysis § IMEI number analysis § SIM number analysis § ISPC number analysis

Quote from International Numbering Plans, ‘Number analysis tools’

No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.

Quote from Association of Chief Police Officers, ‘ACPO Good Practice Guide for Digital Evidence’, March 2012.

Step 1. Securing and Evaluating the Scene: Steps should be taken to ensure the safety of individuals and to identify and protect the integrity of potential evidence. Step 2. Documenting the Scene: Create a permanent record of the scene, accurately recording both digital-related and conventional evidence. Step 3. Evidence Collection: Collect traditional and digital evidence in a manner that preserves their evidentiary value. Step 4. Packaging, Transportation, and Storage: Take adequate precautions when packaging, transporting, and storing evidence, maintaining chain of custody.

Quote from U.S. Department of Justice, ‘Electronic Crime Scene Investigation: A Guide for First Responders’, 2008.

§ Article File: Records on stolen articles and lost public safety, homeland security, and critical infrastructure identification. § Gun File: Records on stolen, lost, and recovered weapons and weapons used in the commission of crimes that are designated to expel a projectile by air, carbon dioxide, or explosive action. § Boat File: Records on stolen boats. § Securities File: Records on serially numbered stolen, embezzled, used for ransom, or counterfeit securities. § Vehicle File: Records on stolen vehicles, vehicles involved in the commission of crimes, or vehicles that may be seized based on federally issued court order. § Vehicle and Boat Parts File: Records on serially numbered stolen vehicle or boat parts. § License Plate File: Records on stolen license plates. § Missing Persons File: Records on individuals, including children, who have been reported missing to law enforcement and there is a reasonable concern for their safety.

Source:
<https://www.fbi.gov/services/cjis/ncic>

§ Foreign Fugitive File: Records on persons wanted by another country for a crime that would be a felony if it were committed in the United States. § Identity Theft File: Records containing descriptive and other information that law enforcement personnel can use to determine if an individual is a victim of identity theft or if the individual might be using a false identity. § Immigration Violator File: Records on criminal aliens whom immigration authorities have deported and aliens with outstanding administrative warrants of removal. § Protection Order File: Records on individuals against whom protection orders have been issued. § Supervised Release File: Records on individuals on probation, parole, or supervised release or released on their own recognizance or during pre-trial sentencing. § Unidentified Persons File: Records on unidentified deceased persons, living persons who are unable to verify their identities, unidentified victims of catastrophes, and recovered body parts. The file cross-references unidentified bodies against records in the Missing Persons File. § Protective Interest: Records on individuals who might pose a threat to the physical safety of protectees or their immediate families. Expands on the U.S. Secret Service Protective File, originally created in 1983. § Gang File: Records on violent gangs and their members. § Known or Appropriately Suspected Terrorist File: Records on known or appropriately suspected terrorists in accordance with HSPD-6. § Wanted Persons File: Records on individuals (including juveniles who will be tried as adults) for whom a federal warrant or a felony or misdemeanor warrant is outstanding. § National Sex Offender Registry File: Records on individuals who are required to register in a jurisdiction's sex offender registry. § National Instant Criminal Background Check System (NICS) Denied Transaction File: Records on individuals who have been determined to be "prohibited persons" according to the Brady Handgun Violence Prevention Act and were denied as a result of a NICS background check. (As of August 2012, records include last six months of denied transactions; in the future, records will include all denials.) § Violent Person File: Once fully populated with data from our users, this file will contain records of persons with a violent criminal history and persons who have previously threatened law enforcement.

Sometimes you will see the following messages in DHCP logs

R. Droms, Network Working Group, March 1997. <https://www.ietf.org/rfc/rfc2131.txt>

Contents at a Glance

- Introduction xxxvii
- 1 The Scope of Digital Forensics 2
- 2 Windows Operating and File Systems 34
- 3 Handling Computer Hardware 92
- 4 Acquiring Evidence in a Computer Forensics Lab 126
- 5 Online Investigations 176
- 6 Documenting the Investigation 224
- 7 Admissibility of Digital Evidence 252
- 8 Network Forensics and Incident Response 314
- 9 Mobile Forensics 372
- 10 Mobile App Investigations 426
- 11 Photograph Forensics 460
- 12 Mac Forensics 480
- 13 Case Studies 538
- 14 Internet of Things (IoT) Forensics and Emergent Technologies 572
- Answer Key 594
- Index 606

Table of Contents

Introduction	xxxvii
Chapter 1: The Scope of Digital Forensics	2
Popular Myths about Computer Forensics	3
Myth 1: Computer Forensics Is the Same As Computer Security	3
Myth 2: Computer Forensics Is about Investigating Computers	3
Myth 3: Computer Forensics Is about Investigating Computer Crime	3
Myth 4: Computer Forensics Is Really Used to Resurrect Deleted Files....	4
Types of Digital Forensic Evidence Recovered	5
Electronic Mail (Email).....	5
Images	7
Video	8
Websites Visited and Internet Searches	9
Cellphone Forensics	10
IoT Forensics.....	10
What Skills Must a Digital Forensics Investigator Possess?	10
Computer Science Knowledge	10
Legal Expertise	11
Communication Skills	11
Linguistic Abilities	12
Continuous Learning.....	12
Programming	12
An Appreciation for Confidentiality	12
The Importance of Digital Forensics	12
Job Opportunities	13
A History of Digital Forensics	14
1980s: The Advent of the Personal Computer.....	15
1990s: The Impact of the Internet.....	15
2000s: Virtual Currencies, IoT, Encryption, and the Edward Snowden Effect	20

Training and Education	21
Law Enforcement Training	21
High School Training.....	22
University Training.....	22
Professional Certifications	22
Summary	27
Key Terms	28
Assessment	30
Chapter 2: Windows Operating and File Systems	34
Physical and Logical Storage	36
File Storage.....	36
Paging	39
File Conversion and Numbering Formats	42
Conversion of Binary to Decimal	42
Hexadecimal Numbering	42
Conversion of Hexadecimal to Decimal.....	43
Conversion of Hexadecimal to ASCII	44
Using Hex to Identify a File Type	47
Unicode.....	47
Operating Systems	47
The Boot Process	48
Windows File Systems.....	49
Windows Registry	59
Registry Data Types.....	61
FTK Registry Viewer.....	62
Microsoft Office	62
Microsoft Windows Features	63
Windows Vista	63
Windows 7	68

Windows 8.1	79
Windows 10	82
Microsoft Office 365.....	83
Summary	84
Key Terms	85
Assessment	88
Chapter 3: Handling Computer Hardware	92
Hard Disk Drives	93
Small Computer System Interface (SCSI).....	93
Integrated Drive Electronics (IDE)	94
Serial ATA (SATA).....	95
Cloning a PATA or SATA Hard Disk	97
Cloning Devices	98
Removable Memory	105
FireWire	105
USB Flash Drives	106
External Hard Drives	107
MultiMediaCards (MMCs)	108
Summary	120
Key Terms	120
Assessment	122
Reference	125
Chapter 4: Acquiring Evidence in a Computer Forensics Lab	126
Lab Requirements	127
American Society of Crime Laboratory Directors (ASCLD).....	127
American Society of Crime Laboratory Directors/Lab Accreditation Board (ASCLD/LAB)	127
ASCLD/LAB Guidelines for Forensic Laboratory Management Practices.....	127

ISO/IEC 17025:2017	129
Scientific Working Group on Digital Evidence (SWGDE)	129
Private-Sector Computer Forensics Laboratories	130
Evidence Acquisition Laboratory	131
Email Preparation Laboratory	131
Inventory Control	131
Laboratory Information Management Systems	131
Web Hosting	132
Computer Forensics Laboratory Requirements	132
Laboratory Layout.....	132
Laboratory Management.....	154
Laboratory Access	155
Extracting Evidence from a Device	157
Using the dd Utility	157
Using Global Regular Expressions Print (GREP)	158
Skimmers	166
Steganography	168
Summary	170
Key Terms	170
Assessment	172
Chapter 5: Online Investigations	176
Working Undercover	177
Generating an Identity.....	178
Generating an Email Account	179
Masking Your Identity	181
Dark Web Investigations	184
OSINT Framework	184
Tor	184

Invisible Internet Project	186
Freenet	186
SecureDrop	186
Dark Web Marketplaces	186
Virtual Currencies	188
Bitcoin	188
Venmo and Vicemo	189
Website Evidence	189
Website Archives	189
Website Statistics	190
Background Searches on a Suspect	191
Finding Personal Information	192
Personal Interests and User Groups	195
Searching for Stolen Property	196
Online Crime	209
Identity Theft	210
Credit Cards for Sale	210
Electronic Medical Records	210
Counterfeit and Counter-proliferation Investigations (CPI)	211
Cyberbullying	211
Social Networking	211
Capturing Online Communications	212
Using Screen Captures	212
Using Video	213
Viewing Cookies	214
Using Windows Registry	215
Edge Web Browser	215
Summary	216
Key Terms	216
Assessment	218

Chapter 6: Documenting the Investigation	224
Obtaining Evidence from a Service Provider	224
Documenting a Crime Scene	226
Seizing Evidence	227
Crime Scene Examinations.....	227
Crime Scene Investigator Equipment	228
Documenting the Evidence.	229
Completing a Chain of Custody Form	229
Completing a Computer Worksheet	230
Completing a Hard Disk Drive Worksheet	232
Completing a Server Worksheet	233
Using Tools to Document an Investigation	234
FragView	234
Helpful Mobile Applications (Apps).....	235
Writing Reports	236
Time Zones and Daylight Saving Time (DST).....	236
Creating a Comprehensive Report	238
Using Expert Witnesses at Trial	242
The Expert Witness.....	242
The Goals of the Expert Witness	242
Preparing an Expert Witness for Trial.....	243
Summary	245
Key Terms	246
Assessment	246
Chapter 7: Admissibility of Digital Evidence	252
History and Structure of the United States Legal System	253
Origins of the U.S. Legal System.....	254
Overview of the U.S. Court System.....	254
In the Courtroom.....	259

Evidence Admissibility	262
Constitutional Law.	262
First Amendment.....	262
First Amendment and the Internet.....	263
Fourth Amendment.....	265
Fifth Amendment.....	279
Sixth Amendment.....	280
Congressional Legislation.....	281
CLOUD (Clarifying Lawful Overseas Use of Data) Act.....	288
Rules for Evidence Admissibility.....	288
Criminal Defense.....	293
California Consumer Privacy Act (CCPA).....	294
NYS DFS Rule 23 NYCRR 500.....	294
Canada Personal Information Protection and Electronic Documents Act (PIPEDA).....	295
When Computer Forensics Goes Wrong.	296
Pornography in the Classroom.....	296
Structure of the Legal System in the European Union (E.U.).	296
Origins of European Law.....	297
Structure of European Union Law.....	297
Privacy Legislation in Asia	303
China.....	304
India.....	304
Summary	305
Key Terms	306
Assessment	309
Chapter 8: Network Forensics and Incident Response	314
The Tools of the Trade.	315
Networking Devices	316

Proxy Servers.....	317
Web Servers.....	317
DHCP Servers.....	321
DHCP Logs.....	323
Hub.....	324
Switch.....	324
SMTP Servers.....	324
DNS Servers.....	326
The Hosts File.....	327
DNS Protocol.....	328
Internet Corporation for Assigned Names and Numbers (ICANN).....	328
Traceroute.....	328
Routers.....	328
IDS.....	338
Firewalls.....	339
Ports.....	340
Understanding the OSI Model	341
The Physical Layer.....	341
The Data Link Layer.....	342
The Network Layer.....	342
The Transport Layer.....	343
The Session Layer.....	344
The Presentation Layer.....	344
The Application Layer.....	345
Introduction to VoIP.	346
Voice over Internet Protocol (VoIP).....	346
Disadvantages of VoIP.....	346
PBX (Private Branch Exchange).....	346

Session Initiation Protocol (SIP).....	348
STUN (Simple Traversal of UDP Through NATs (Network Address Translation)).....	348
Incident Response (IR)	348
STIX, TAXII, and Cybox	349
Advanced Persistent Threats	349
APT10	350
Cyber Kill Chain	350
Indicators of Compromise (IOC)	354
Investigating a Network Attack	357
Random Access Memory (RAM).....	357
AmCache	357
ShimCache.....	358
ShellBags.....	358
Volume Shadow Copy	358
Endpoint Detection and Response (EDR).....	359
Kibana.....	359
Log2Timeline/Plaso	359
SANS SIFT Workstation	360
Windows Registry	361
Summary	364
Key Terms	365
Assessment	367
Chapter 9: Mobile Forensics	372
The Cellular Network	374
Base Transceiver Station	374
Mobile Station.....	378
Cellular Network Types	383
SIM Card Forensics	385
Types of Evidence.....	388

Handset Specifications	389
Memory and Processing	389
Battery.....	390
Other Hardware.....	390
Mobile Operating Systems	391
Android OS	391
Symbian OS.....	400
BlackBerry 10.....	400
Windows Phone	400
Standard Operating Procedures for Handling Handset Evidence.	401
National Institute of Standards and Technology (NIST)	401
Handset Forensics.	406
Cellphone Forensics Tools.....	406
Logical Versus Physical Examination.....	408
Manual Cellphone Examinations	408
Flasher Box.....	409
Global Satellite Service Providers	410
Satellite Communication Services	410
Legal Considerations	410
National Crime Information Center (NCIC).....	411
Other Mobile Devices	413
Tablets.....	413
GPS Tracking	414
Documenting the Investigation.	415
Summary	416
Key Terms	416
Assessment	421

Chapter 10: Mobile App Investigations	426
Static Versus Dynamic Analysis	427
Static Analysis.....	427
Dynamic Analysis.....	431
Introduction to Debookee	433
Dating Apps	441
Tinder	442
Grindr	445
Rideshare Apps	450
Uber	451
Communication Apps	453
Skype	453
Summary	457
Key Terms	457
Assessment	458
Chapter 11: Photograph Forensics	460
National Center for Missing and Exploited Children (NCMEC)	462
Project VIC	463
Case Studies	463
Facebook Selfie	463
To Catch a Predator	463
Extortion.....	464
Understanding Digital Photography.	464
File Systems.....	464
Digital Photography Applications and Services.....	465
Examining Picture Files.	466
Exchangeable Image File Format (EXIF)	467
Evidence Admissibility	470

Federal Rules of Evidence (FRE).....	470
Analog vs. Digital Photographs.....	470
Case Studies	471
Worldwide Manhunt.....	471
NYPD Facial Recognition Unit.....	473
Summary	474
Key Terms	474
Assessment	475
Chapter 12: Mac Forensics	480
A Brief History	480
Macintosh.....	481
Mac mini with OS X Server.....	481
iPod.....	482
iPhone.....	483
iPad.....	485
iPad Pro.....	485
Apple Watch.....	485
Apple Wi-Fi Devices	487
Apple TV.....	487
AirPort Express.....	488
AirPort Extreme.....	488
AirPort Time Capsule.....	488
Macintosh File Systems	489
Hierarchical File System (HFS).....	489
HFS+.....	489
APFS.....	490
Forensic Examinations on a Mac.....	494
Epoch Time.....	496
DMG.....	498

PList Files.....	499
SQLite Databases	501
Email Files.....	501
Hibernation File.....	501
Macintosh Operating Systems	502
macOS Catalina.....	502
File Vault.....	503
Disk Utility	503
macOS Keychain	503
iCloud Keychain.....	504
Multiple Displays.....	504
Notifications	504
Tags.....	504
Safari.....	504
Target Disk Mode and Device Cloning.....	506
Apple Mobile Devices	507
iOS	508
Enterprise Deployment of Apple Devices	526
Battery.....	527
Performing a Mac Forensics Examination.	527
Case Studies	529
Find My iPhone.....	529
Wanted Hactivist.....	529
Michael Jackson	529
Stolen iPhone.....	529
Drug Bust.....	530
Murder Trial	530
Summary	531
Key Terms	531
Assessment	535

Chapter 13: Case Studies	538
Silk Road	538
Genesis of the Silk Road.....	539
Death Threat	542
Silk Road Takedown	542
The Takedown of Ulbricht	543
Ross Ulbricht Pre-trial.....	544
Ross Ulbricht on Trial.....	546
Laptop Evidence.....	546
Trial Verdict.....	549
Las Vegas Massacre	549
Zacharias Moussaoui	551
Background.....	551
Digital Evidence	552
Standby Counsel Objections	553
Prosecution Affidavit.....	554
Exhibits	554
BTK (Bind Torture Kill) Serial Killer	555
Profile of a Killer	555
Evidence	556
Cyberbullying	557
Federal Anti-harassment Legislation	557
State Anti-harassment Legislation.....	557
Warning Signs of Cyberbullying.....	557
What Is Cyberbullying?.....	558
Phoebe Prince.....	558
Ryan Halligan	559
Megan Meier	559
Tyler Clementi	559

Sports	561
Summary	563
Key Terms	563
Assessment	564
Assignment	570
Chapter 14: Internet of Things (IoT) Forensics and Emergent Technologies	572
5G	573
Wi-Fi 6	575
Wi-Fi Mesh Networks	576
Shodan	576
Mirai Botnet	577
Cryptocurrency Mining	577
Alexa	578
Micro-Chipping	579
Fitness Trackers	579
Apple Watch	581
Action Cameras	583
Police Safety	583
Police Vehicles	585
Vehicle Forensics	585
Low-Tech Solution for High-Tech Seizures	586
Summary	588
Key Terms	588
Assessment	590
Answer Key	594
Index	606

About the Author

Dr. Darren R. Hayes is a leading expert in the field of digital forensics and computer security. He is the Director of Digital Forensics and Associate Professor at Pace University, and he has been named one of the Top 10 Computer Forensics Professors by Forensics Colleges. He was selected as the recipient of the *2020 Homeland Security Investigations New York Private Sector Partnership Award*.

During his time at Pace University, Hayes developed a Digital Forensics track for the University's Bachelor of Science in Information Technology degree in addition to his development of digital forensics graduate courses. He also created, and now manages, the Pace University Digital Forensics Research Laboratory, where he devotes most of his time to working with a team of students to support the efforts of law enforcement and the University's students. As part of his research and promoting this scientific field of study, he has fostered relationships with the New York Police Department, New York County D.A., Westchester County D.A., Homeland Security Investigations, National Crime Agency and numerous other agencies.

Hayes is not only an academic, however—he is also a practitioner. He has been an investigator on both civil and criminal investigations and frequently consults on cases for law firms. In fact, he has been declared an expert witness in U.S. federal court.

In New York City, Hayes has been working with six to eight public high schools to develop a curriculum in computer forensics and cybersecurity. He collaborates on computer forensics projects internationally and served as an extern examiner for the MSc in the Forensic Computing and Cybercrime Investigation degree program at University College Dublin for four years.

Hayes has appeared on CNBC, Bloomberg Television, MSNBC and Fox News and been quoted by *Associated Press*, *CNN*, *Wall Street Journal*, *The Guardian (UK)*, *The Irish Independent*, *Japan Times*, *Investor's Business Daily*, *MarketWatch*, *Newsweek*, *SC Magazine*, *Silicon Valley Business Journal*, *USA Today*, *Washington Post*, and *Wired News*. His op-eds have been published by Homeland Security Today, USA Today, and The Hill's Congress Blog. In addition, he has authored a number of peer-reviewed articles in many prominent academic journals. Hayes has been both an author and reviewer for Pearson Prentice Hall since 2007.

About the Technical Reviewers

Lorne Dannenbaum has been working in digital forensics since 2004. He is an experienced Cyber-Security Analyst with a demonstrated history of working in the information technology and services industry. Skilled in Digital Forensics and Incident Response, he performed examinations of systems regarding incidents such as intrusions, data loss protection, malware, and fraud. He uses skills such as memory analysis, file system, and artifact analysis to conduct digital forensic examinations using a wide variety of tools.

Amir Lakhani is a leading senior security strategist. He is responsible for providing IT security solutions to major enterprises and government organizations. Mr. Lakhani creates technical security strategies and leads security implementation projects for Fortune 500 companies. He has designed

offensive counter-defense measures for the Department of Defense and national intelligence agencies, as well as Global 100 organizations. He has also assisted organizations with safeguarding IT and physical environments from attacks perpetrated by underground cybercriminal groups. Mr. Lakhani is considered an industry leader for creating detailed security architectures within complex computing environments. His areas of expertise include cyber defense, mobile application threats, malware management, Advanced Persistent Threat (APT) research, and investigations relating to the Internet's dark security movement. He is the author or contributor of several books and has appeared on FOX Business News, National Public Radio, and other media outlets as an expert on cybersecurity.

Dedication

*This book is dedicated to my loving wife, Nalini, and my children,
Shay, Fiona, Aine, and Nicolai.*

*I also dedicate this book to law enforcement, first responders, and our
military veterans, who risk their lives to protect our safety.*

Acknowledgments

I should begin by acknowledging my supportive and patient wife, Nalini, who is my best friend. Long hours working on a book mean sacrifices for everyone in the family, and my children, Nicolai, Aine, Fiona, and Shay, have been brilliant. My parents, Annette and Ted, have been mentors throughout my life, and I will always be in their debt.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@informit.com

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

The field of digital forensics has grown immensely and diversified over the past few years for a number of reasons. Therefore, this book addresses these changes in a number of new and existing chapters. The proliferation of IoT devices, wearable technologies and other new technologies, like 5G, are explained in detail in Chapter 14 because their impact on digital forensics will be profound. The chapter also discusses how new technologies are changing policing and the safety of law enforcement officers. The chapter also discusses the growing field of vehicle forensics.

There has been no slowdown in the number of network breaches globally; therefore, the need for digital forensics examiners in incident response is greater than ever. Therefore, Chapter 8 is focused on developing the skills of incident responders and highlighting indicators of compromise.

Mobile forensics continually changes and these changes are addressed in numerous chapters, including Chapter 7, when some Supreme Court landmark decisions have changed the rules for law enforcement. Chapter 9 provides an introduction to Mobile Forensics but also explains the changes in Android devices and methods of examination. Chapter 12 explains how iPhone examinations have changed dramatically and shows how full file system extractions are now available with a recently discovered exploit. Mobile applications (apps) save an immense amount of personal information and pretty much every investigation includes at least one mobile device. Therefore, Chapter 10 is a new chapter that provides investigators with forensic techniques to perform both a static and a dynamic examination of mobile apps. Furthermore, this chapter explains how real-time intelligence can be gathered from many popular apps.

Every chapter has been updated extensively to incorporate many recent changes in technology and newly discovered techniques to obtain digital evidence.

This book assumes no prior knowledge of the subject matter, and I have written it for both high school and university students and professional forensics investigators. Additionally, other professions can clearly benefit from reading this book—it is useful for lawyers, forensic accountants, security professionals, and others who have a need to understand how digital evidence is gathered, handled, and admitted to court. The book places a significant emphasis on process and adherence to the law, which are equally important to the evidence that can ultimately be retrieved.

The reader of this book should also realize that comprehensive knowledge of computer forensics can lead to a variety of careers. Digital forensics examiners and experts work for accounting firms, software companies, banks, law enforcement, intelligence agencies, and consulting firms. Every major company has an incident response team and many have a threat intelligence team or department. This book will certainly benefit those in that profession or perhaps those considering a career change. The growth of social media and open source data and tools creates a wealth of information for investigators and these are discussed in the book. Some are experts in mobile forensics, some excel in network forensics, and others focus on personal computers. Other experts specialize in Mac forensics or reverse engineering malware. The good news for graduates with computer forensics experience is that they have a variety of directions to choose from: the job market for them will remain robust, with more positions than graduates for the foreseeable future.

This book is a practical guide, not only because of the hands-on activities it offers, but also because of the numerous case studies and practical applications of computer forensics techniques. Case studies are a highly effective way to demonstrate how particular types of digital evidence have been successfully used in different investigations.

Finally, this book often refers to professional computer forensics tools that can be expensive. You should realize that academic institutions can take advantage of significant discounts when purchasing these products. The book makes a point of mentioning many free or low-cost forensics tools that can be just as effective as some of the expensive tools. You can definitely develop your own program or laboratory in a budget-conscious way.

Register this book to unlock the data files that are needed to complete the end-of-chapter projects.

Follow the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789759917.
3. Click on the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This page intentionally left blank

Chapter 10

Mobile App Investigations

Learning Outcomes

After reading this chapter, you will be able to understand the following:

- The importance of mobile apps in investigations;
- How to perform a static and dynamic analysis;
- The digital evidence available from dating, rideshare, and other popular apps;
- The value of deep-linking in investigations; and
- Analyzing SQLite databases.

Mobile applications (apps) are extremely important today in investigations for a variety of reasons. Interestingly, the databases associated with many apps, are unencrypted and are not too difficult to analyze. Furthermore, if a mobile device is locked or inaccessible, there are many other options available, which may include analyzing a linked desktop version of the app or sending a subpoena, or court order, to a third-party provider to obtain a suspect's data. Third-party companies collect, and store, a tremendous amount of data on their customers. Finally, many users opt to back up their data to cloud storage. For example, WhatsApp has the option for Apple iPhone/iPad users to back up their chats to iCloud, and that backup can be requested from Apple. Nevertheless, organized criminals and terrorist groups largely use mobile apps that utilize strong encryption or proprietary encryption, which can seriously hamper the work of law enforcement. Compounding these concerns is the fact that many apps maintain their servers in countries like Russia, which is beyond the reach of law enforcement in the West. Popular communication apps that use strong encryption include Telegram, Signal, Wickr, and Threema to name but a few. Nevertheless, zero-day exploits are frequently found in mobile apps, including Telegram, which can help investigators to gain access to an encrypted app. A **zero-day exploit** is a security vulnerability that is a threat on the day that it is discovered because a software patch, to fix the exploit, does not yet exist.

Static Versus Dynamic Analysis

During app installation, typically a SQLite database will be installed on the user device. This is a relational database that is comprised of tables. The data stored in these tables may or may not be encrypted. A table may contain a user's contacts, while a related table may store communications with contacts, for example. It is important to understand that these databases contain an extraordinary amount of personal information and, when unencrypted, can put an individual at risk for social engineering. Additionally, we should always consider the possibility to subpoena a third-party service provider for evidence.

When analyzing mobile apps, there are several approaches that an investigator can take, in order to examine the user data. A static analysis includes an examination of the SQLite database associated with that app. A dynamic analysis of the app is an analysis of the behavior of the application once it has been executed (or run). The sections that follow examine static analysis and dynamic analysis in more detail.

Static Analysis

A SQLite database is a relational database that is the preferred storage for data associated with mobile apps. SQLite is a C-language library that is responsible for the SQL database. SQLite source code is source code that resides in the public domain. Forensic tools, like BlackLight, enable the user to easily browse through application SQLite databases but there are other standalone tools that can be used. One of these tools is SQLite Database Browser, which is freeware. Later in this chapter we shall detail the types of evidence available from a number of popular mobile apps. Figure 10.1 shows an example of a SQLite database for the Tinder app on an iPhone.

Name	Date Created	Date Modified
com.cardify.tinder	2019-02-08 15:16:59 (UTC)	2019-02-08 15:17:13 (UTC)
Documents	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:14 (UTC)
Library	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:12 (UTC)
Application Support	2019-02-08 15:17:26 (UTC)	2019-02-26 15:26:53 (UTC)
com.crashlytics	2019-02-08 15:17:26 (UTC)	2019-02-08 15:17:26 (UTC)
GoogleMobileAds	2019-02-26 15:26:53 (UTC)	2019-06-20 15:35:12 (UTC)
io.branch	2019-02-08 15:17:30 (UTC)	2019-06-20 15:35:12 (UTC)
Tinder	2019-02-08 15:17:27 (UTC)	2019-02-26 15:26:50 (UTC)
Tinder2.sqlite	2019-02-08 15:17:27 (UTC)	2019-06-20 15:33:18 (UTC)
com-accountkit-sdk-AppEvents...	2019-04-03 14:04:10 (UTC)	2019-04-03 14:04:10 (UTC)
com-accountkit-sdk-PersistedA...	2019-02-08 15:17:49 (UTC)	2019-02-08 15:17:49 (UTC)
com-facebook-sdk-AppEventsP...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-AppEventsT...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-PersistedAn...	2019-02-08 15:17:30 (UTC)	2019-02-08 15:17:30 (UTC)
Cookies	2019-02-20 16:44:23 (UTC)	2019-06-20 15:35:13 (UTC)
Preferences	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:23 (UTC)
WebKit	2019-02-20 16:44:23 (UTC)	2019-02-20 16:44:23 (UTC)

FIGURE 10.1 Tinder SQLite database on iOS (iPhone)

A cursory view of the information in Figure 10.1 shows that there are many folders and files associated with a mobile app SQLite database. Ultimately, the database could have five tables or could have 100 tables, which means that a thorough examination can be a painstaking process. Within each SQLite database (*.sqlite*) you will find databases, which will contain the file extension *.db*; for example, *google_analytics.db*. You will often find recognizable files, like *.jpg* (picture images), *.vcf* (or vCard for your contacts), or *.mp3* (sound file).

The chart in Figure 10.2 provides a general outline of how an iOS application is stored on an iPhone or iPad.

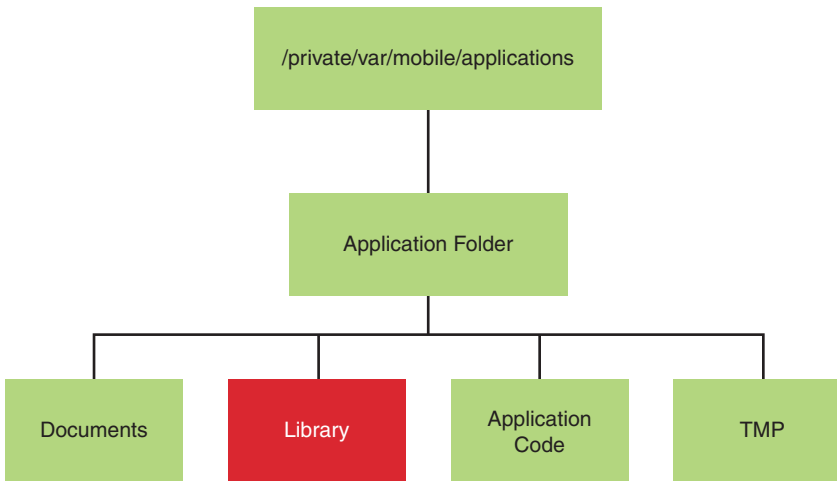


FIGURE 10.2 Application storage on iOS

The **Library** folder, which is highlighted in Figure 10.2, is where you will find the all-important user data, including cache, cookies, and other personal information. In the **Preferences** folder, which is displayed and highlighted in Figure 10.3, you may actually discover usernames and passwords that are stored in plaintext.

In Figure 10.4, we can view the name *com.cardify.tinder* and this is referred to as a bundle ID. A **bundle ID** is a uniform type identifier, which is comprised of alphanumeric characters, that uniquely identifies a specific app. The bundle ID for Microsoft’s iOS Outlook app is *com.microsoft.Office.Outlook*. Thus, the format for the bundle ID is generally *com.<YourCompany>.<AppName>*, which is referred to as a reverse-domain name style string. When you visit the Apple App Store and search for the Microsoft Outlook app for iOS, then you will arrive at this URL in your web browser: <https://apps.apple.com/us/app/microsoft-outlook/id951937596>. Notice the “id951937596”, which identifies this app on the App Store. An iOS app also has a unique identifier known as an App ID. An **App ID** is a two-part string that identifies a development team (Team ID) and an application (bundle ID). The Team ID is created and assigned by Apple, while the bundle ID is generated by the app developer.

Name	Date Created	Date Modified
com.cardify.tinder	2019-02-08 15:16:59 (UTC)	2019-02-08 15:17:13 (UTC)
Documents	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:14 (UTC)
Library	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:12 (UTC)
Application Support	2019-02-08 15:17:26 (UTC)	2019-02-26 15:26:53 (UTC)
com.crashlytics	2019-02-08 15:17:26 (UTC)	2019-02-08 15:17:26 (UTC)
GoogleMobileAds	2019-02-26 15:26:53 (UTC)	2019-06-20 15:35:12 (UTC)
io.branch	2019-02-08 15:17:30 (UTC)	2019-06-20 15:35:12 (UTC)
Tinder	2019-02-08 15:17:27 (UTC)	2019-02-26 15:26:50 (UTC)
Tinder2.sqlite	2019-02-08 15:17:27 (UTC)	2019-06-20 15:33:18 (UTC)
com-accountkit-sdk-AppEvents...	2019-04-03 14:04:10 (UTC)	2019-04-03 14:04:10 (UTC)
com-accountkit-sdk-PersistedA...	2019-02-08 15:17:49 (UTC)	2019-02-08 15:17:49 (UTC)
com-facebook-sdk-AppEventsP...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-AppEventsT...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-PersistedAn...	2019-02-08 15:17:30 (UTC)	2019-02-08 15:17:30 (UTC)
Cookies	2019-02-20 16:44:23 (UTC)	2019-06-20 15:35:13 (UTC)
Preferences	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:23 (UTC)
WebKit	2019-02-20 16:44:23 (UTC)	2019-02-20 16:44:23 (UTC)

FIGURE 10.3 Tinder SQLite database on iOS

Name	Date Created	Date Modified
com.cardify.tinder	2019-02-08 15:16:59 (UTC)	2019-02-08 15:17:13 (UTC)
Documents	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:14 (UTC)
Library	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:12 (UTC)
Application Support	2019-02-08 15:17:26 (UTC)	2019-02-26 15:26:53 (UTC)
com.crashlytics	2019-02-08 15:17:26 (UTC)	2019-02-08 15:17:26 (UTC)
GoogleMobileAds	2019-02-26 15:26:53 (UTC)	2019-06-20 15:35:12 (UTC)
io.branch	2019-02-08 15:17:30 (UTC)	2019-06-20 15:35:12 (UTC)
Tinder	2019-02-08 15:17:27 (UTC)	2019-02-26 15:26:50 (UTC)
Tinder2.sqlite	2019-02-08 15:17:27 (UTC)	2019-06-20 15:33:18 (UTC)
com-accountkit-sdk-AppEvents...	2019-04-03 14:04:10 (UTC)	2019-04-03 14:04:10 (UTC)
com-accountkit-sdk-PersistedA...	2019-02-08 15:17:49 (UTC)	2019-02-08 15:17:49 (UTC)
com-facebook-sdk-AppEventsP...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-AppEventsT...	2019-06-20 15:35:12 (UTC)	2019-06-20 15:35:12 (UTC)
com-facebook-sdk-PersistedAn...	2019-02-08 15:17:30 (UTC)	2019-02-08 15:17:30 (UTC)
Cookies	2019-02-20 16:44:23 (UTC)	2019-06-20 15:35:13 (UTC)
Preferences	2019-02-08 15:16:59 (UTC)	2019-06-20 15:35:23 (UTC)
WebKit	2019-02-20 16:44:23 (UTC)	2019-02-20 16:44:23 (UTC)

FIGURE 10.4 Tinder SQLite database on iOS

Static Analysis: Code Review

Another form of static analysis refers to performing a code review on a mobile app, which can help the investigator understand the type of evidence that is available. In terms of the evidence available for an Android app (.apk or Android Package) there is the manifest, which shows the permissions associated with a particular app. For example, the manifest may show that the app is collecting user location information (“COARSE_LOCATION” and/or “FINE_LOCATION”). ACCESS_COARSE_LOCATION is a permission that enables the app to access the approximate location of the user device, which is based on NETWORK_PROVIDER (cell sites, i.e. cell towers). ACCESS_FINE_LOCATION enables the app to determine the location of the user device based on NETWORK_PROVIDER and GPS (GPS_PROVIDER). An Android application contains a file at the root of the project source set, which is

called *AndroidManifest.xml*. An **Android manifest file** contains the application's package name, its functionality, permissions, hardware, and software requirements for installation.

Understanding the permissions associated with an app allows the investigator to understand the type of evidence that can be requested from the provider and the type of evidence to look for when examining the SQLite database. The latter is important because examining one database can take many days, or even weeks, and therefore limiting the scope of your analysis is key. Example 10.1 shows a small extract from an Android manifest for WhatsApp.

EXAMPLE 10.1 Android Permissions Manifest for WhatsApp

```
<manifest xmlns:"http://schemas.android.com/apk/res/android"
android:versionCode="451048" android:versionName="2.12.550" package="com.whatsapp"
platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767" >
  <uses-sdk android:minSdkVersion="7" android:targetSdkVersion="23" />
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
  <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS" />
  <uses-permission android:name="android.permission.BLUETOOTH" />
  <uses-permission android:name="android.permission.BROADCAST_STICKY" />
  <uses-permission android:name="android.permission.CAMERA" />
  <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
  <uses-permission android:name="android.permission.GET_ACCOUNTS" />
  <uses-permission android:name="android.permission.GET_TASKS" />
  <uses-permission android:name="android.permission.INSTALL_SHORTCUT" />
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.MANAGE_ACCOUNTS" />
  <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS" />
  <uses-permission android:name="android.permission.READ_CONTACTS" />
  <uses-permission android:name="android.permission.READ_PHONE_STATE" />
```

An understanding of the manifest is also important from a mobile security perspective. Many privacy policy statements are misleading or confusing and provide poor guidance about how trustworthy a mobile app is. The Federal Trade Commission (FTC), for example, investigated a popular free app for Android, called the Brightest Flashlight, after it was discovered that the app requested many more permissions from the user's device beyond the light function on the device. Therefore, some app permissions are high risk, while other permissions are low risk.

A Web search for the "Uber APK file", or any other APK file, quickly identifies where the application package can be downloaded. Once the APK has been downloaded, there are a number of applications that can be used to review the code and manifest for the APK. One tool for reviewing the APK developer code is dex2jar (dex compiler), which can be downloaded from SourceForge. Another application for viewing the APK is FileViewer Plus. One preferred tool is an online Java APK decompiler application,

which is available from www.javadecompilers.com/apk. With this tool, you can decompile your APK in a web browser without downloading an APK decompiler to your computer. Therefore, you do not need to worry whether the application that you are downloading is from a trusted source because the application is being run from their web server and not from your computer. There are numerous other source code analytical tools that an investigator can use, including SourceMeter, JSLint, and FindBugs. Figure 10.5 shows the JSLint user interface.



FIGURE 10.5 JSLint user interface

Dynamic Analysis

A dynamic analysis of the app is an analysis of the behavior of the application once it has been executed (or run). An **Android emulator** is an application that simulates, or runs, the Android operating system in a virtual machine. These applications are generally developed for use with a personal computer and run as a virtual machine. App developers use an emulator to analyze how their apps will run before making them available to the public. However, an emulator can also benefit investigators who are interested in viewing the behavior of an app—especially if an app potentially contains malware. This is the benefit of using an emulator that operates as a virtual machine. An investigator may also be interested in monitoring the permissions and DNS connections associated with an executed mobile app. In terms of monitoring DNS connections (connections to servers), there is Wireshark (Windows) and Debookee (macOS), which are very effective at monitoring these connections over a wireless network. Figure 10.6 shows a screenshot of a pcap (packet capture) file from Wireshark. A **pcap file** is a wireless packet that contains user data and network data related to the sender and receiver of that data.

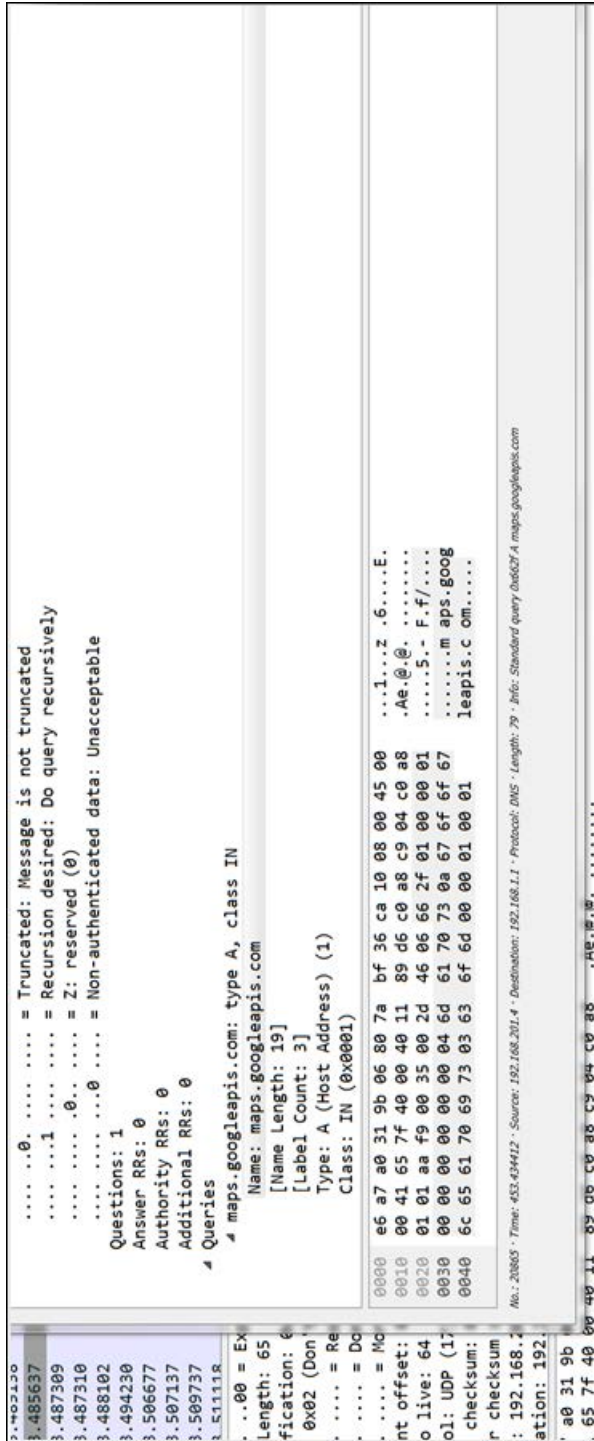


FIGURE 10.6 Google Maps API identified in a PCAP captured by Wireshark

Note

When performing any type of wireless monitoring, ensure that you have permission to be on a particular network and ensure that you are only monitoring your wireless traffic.

To remain safe and compliant, consider using a personal hotspot device, like a Verizon Jetpack, in a secure lab. A tool like Debookee also has the ability to encrypt some wireless traffic, which means that while app data may be encrypted on the device and on the server, often companies will implement poor encryption protocols, whereby the data in transmission can be intercepted and viewed in plaintext. Thus, tools like Debookee can also be used, by security professionals analyzing apps, to try to determine how secure apps are.

Introduction to Debookee

Debookee is a comprehensive wireless packet sniffer for macOS. The tool is not passive as it performs a man-in-the-middle (MITM) attack to intercept data from mobile and IoT devices. A **man-in-the-middle (MITM) attack** is an attempt to intercept electronic communications between two computing devices, with the intent to decipher encrypted messages. The tool also performs SSL/TLS decryption. Debookee supports numerous protocols, including HTTP, HTTPS, DNS, TCP, DHCP, SIP, and RTP (VoIP). The tool can be used to identify what data is being collected and shared by mobile apps. In other words, you can identify DNS connections to servers around the world and other companies that could be potentially subpoenaed for information. The data generated from one mobile app can be shared with fifty or more third-party companies, which are mostly analytics companies like Crashlytics, UXCam, Fabric, etc.

On the homepage of the Debookee website, click the **Download** button and install the software.

Note

You do not need to purchase the software but can begin by using the trial version. You may of course later decide to purchase the software, which is relatively inexpensive, and one license can be used on two different computers.

Once you install the software and start the program, you will see an interface, similar to Figure 10.8. The IP address, MAC address, and host name that are displayed provide information about your device.

Figure 10.9 shows a close-up of the information that we just discussed. Click the **Start LanScan** button as highlighted in Figure 10.9.



FIGURE 10.7 Debookee home page

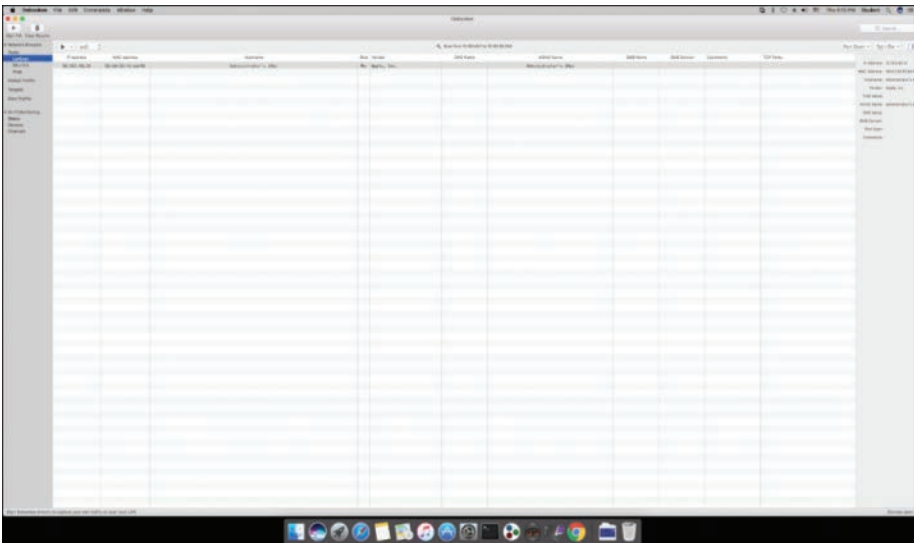


FIGURE 10.8 Debookee user interface

You will then see a list of all devices that are connected to the same wireless access point as your computer. Once you select your target device, click the **Pcap** option, on the upper left of your screen, and then click **Save Pcap files**, as shown in Figure 10.10.

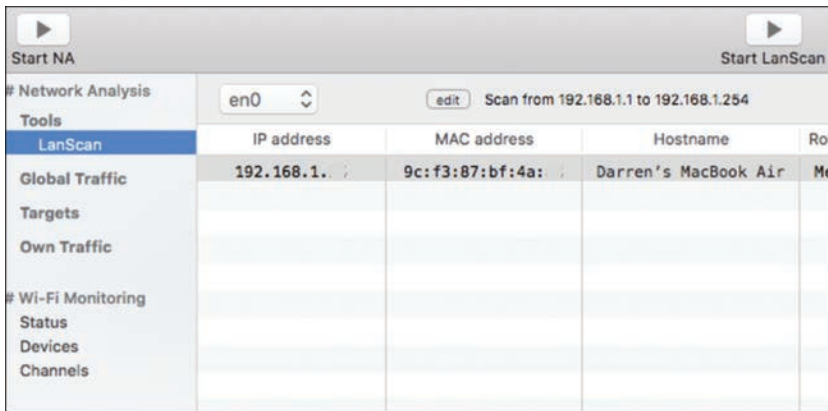


FIGURE 10.9 Debookee user interface with host computer information displayed

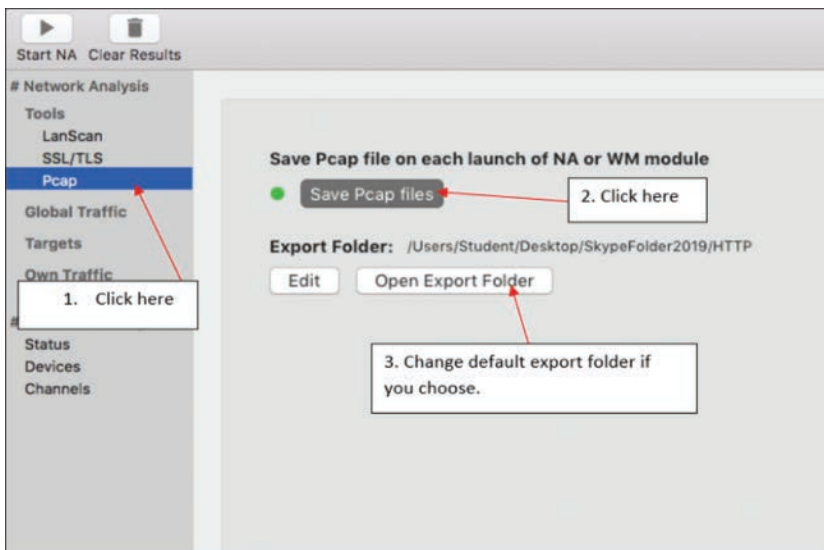


FIGURE 10.10 Save Pcap files option in Debookee

You can then click the **Open Export Folder** button to change the default export folder. There is an add-on tool in Debookee, which allows you to decrypt the contents of the pcap files. If you purchase this option, you can click the **SSL/TLS** button displayed in Figure 10.11.

The next step in the TLS decryption process is to install the certificate authority (CA) on the machine (see Figure 10-12). To start your NA, click the Play button ► in the very top left of your application screen (underneath it says, "Start NA"). Once the trust certificate has been installed, you should stop the NA (Network Analysis) by clicking the same button.

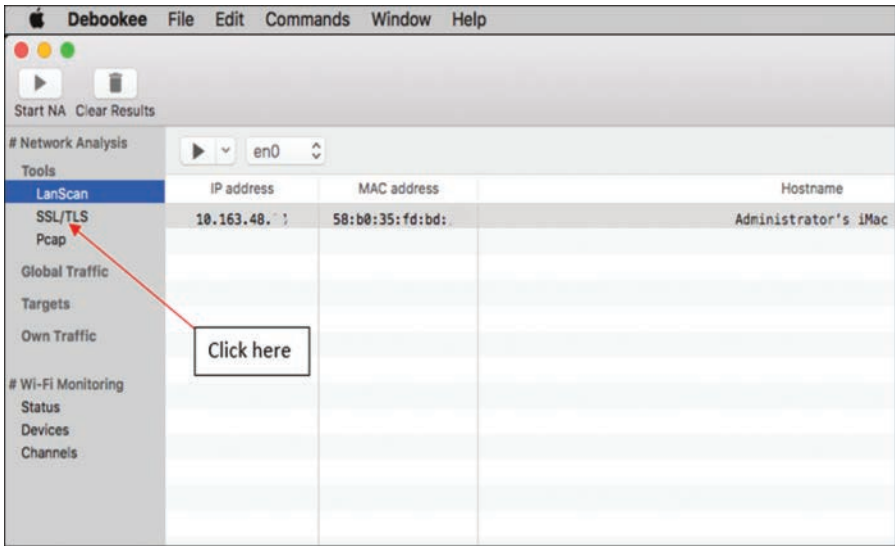


FIGURE 10.11 SSL/TLS decryption option in Debookee

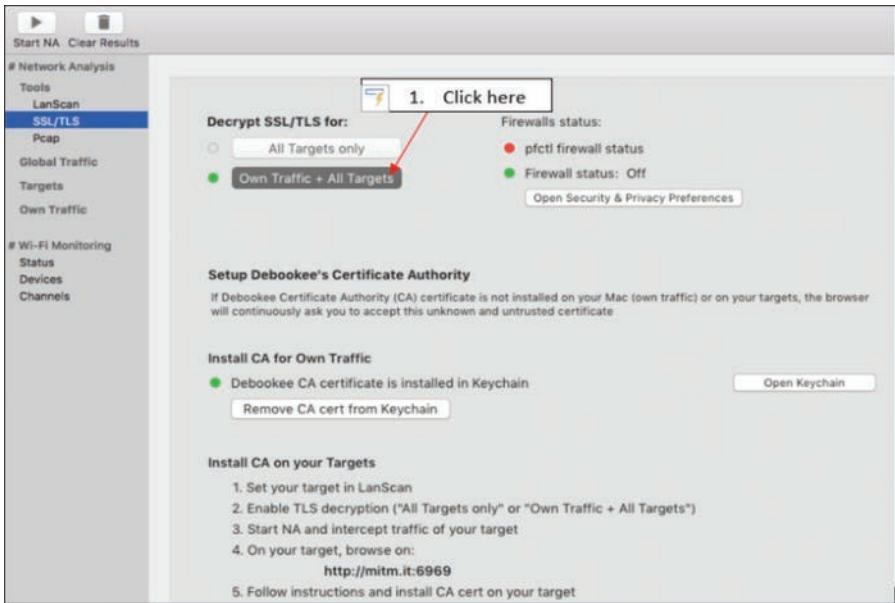


FIGURE 10.12 Decryption option in Debookee

From the screen in Figure 10.13, click the **Start NA** ► button again. Open the webpage, or application, you want to analyze (or the device that you wish to monitor), and begin generating data packets by opening and closing different functions, sending messages, or just using the application.

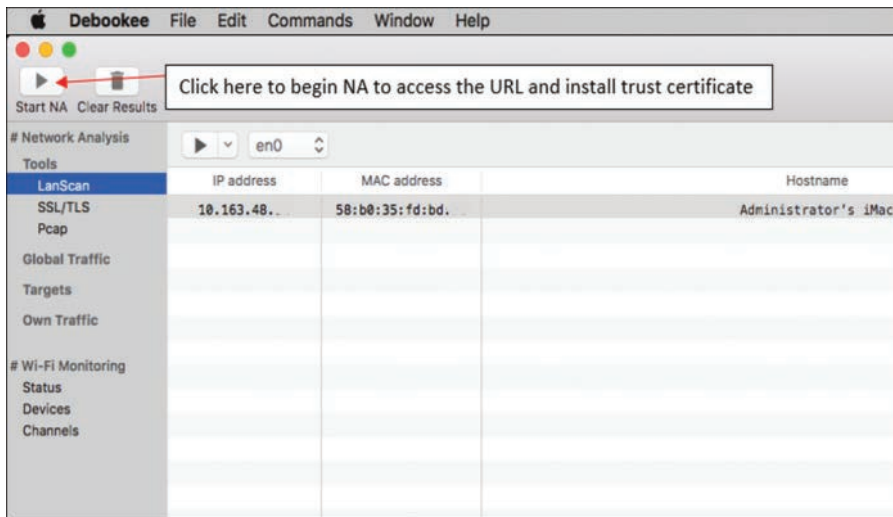


FIGURE 10.13 Start NA option in Debookee

On the left column in Figure 10.14, under **Own Traffic**, you will see that **DNS** and **HTTP** have populated. The NA will run continuously until you terminate it. When you are satisfied with the data collected, press the stop button. Remember that your pcap files are automatically exported to the folder that you previously selected.

Click **DNS** in the left column and you will see all DNS connections made during the NA (timestamped) with the hostname and/or IP address. These are the IP addresses and hosts that you can analyze, in addition to the pcaps.

It is recommended that you click **File > Export** and save this list as a .doc or a .txt file. You can then use some open source DNS analysis tools, including www.robtext.com and www.dnsdumpster.com.

Clicking the **HTTP** button, as shown in Figure 10.15, will display an itemized list of every packet transmitted over HTTP, HTTPS, TCP, SIP, IMAP, and other protocols. If you did not purchase the SSL/TLS decrypt module, HTTPS packets (transmitted over port 443 using TLSv1.2) will display in red, and you will not be able to read the data until you decrypt the packets. Port 443 is the port number for secure HTTP communications—in other words, Web traffic. If you did purchase the SSL/TLS decrypt module, HTTPS packets will display in black, and when you click on them, the data will be displayed in plaintext in the data field.

Click on a packet that you wish to examine. In the data field you will see some text populate underneath the tab labeled **Request**. Upon further inspection of the data field, you will see the full GET request along with the packet parameters and data, as displayed in Figure 10.16. **GET** is an HTTP method used to request data from a specific resource, like a web server.

# Network Analysis	Time	Hostname	IP
Tools	16:19:12	lh3.googleusercontent.com	172.217.12.129
LanScan	16:19:12	www.gstatic.com	172.217.12.163
SSL/TLS	16:19:12	lh5.googleusercontent.com	172.217.12.129
Pcap	16:19:12	encrypted-tbn3.gstatic.com	172.217.12.206
Global Traffic	16:19:13	www.facebook.com	31.13.71.36
Targets	16:19:13	static.xx.fbcdn.net	31.13.71.7
Own Traffic	16:19:13	scontent-lga3-1.xx.fbcdn.net	31.13.71.7
DNS	16:19:14	googleads.g.doubleclick.net	172.217.12.194
HTTP	16:19:37	www.instagram.com	31.13.71.174
	16:19:39	connect.facebook.net	31.13.71.7
# Wi-Fi Monitoring	16:19:41	clients1.google.com	172.217.6.206
Status	16:19:41	graph.instagram.com	31.13.71.52

FIGURE 10.14 DNS connections captured

# Network Analysis	Time	URL	Method	Size
Tools	13:05:06	http://v16.muscdn.com/d2f41c7f2580685ec5398488659d1ac2/Se2791bd/video/tos/maliva/tos-maliva-v-0068/3ff13...	GET	206
LanScan	13:05:06	http://v16.muscdn.com/fcc95ee17db0475430c9c5193291a5bc/Se2791ba/video/tos/useast2a/tos-useast2a-ve-0068...	GET	206
	13:05:07	http://v16.muscdn.com/f0456678af5159bb248719715a689e79/Se2791b7/ideo/tos/maliva/tos-maliva-v-0068/1ddc...	GET	206
	13:05:08	http://v16.muscdn.com/df98407dbd3d4afd1d80bb7f8c1129a0/Se2791bb/video/tos/maliva/tos-maliva-v-0068/ff341...	GET	206
Targets	13:05:14	http://p16.muscdn.com/img/tos-maliva-p-0068/c0ac737d1b2d4beb8aacdf1db04d110_1574604937-tpiv-tiktok-shrL...	GET	200
192.168.2.3	13:05:14	http://p16.muscdn.com/img/tos-maliva-p-0068/bdcca8b537744038907158e027fdb33_1574555997-tpiv-tiktok-shrL...	GET	200
HTTP	13:05:14	http://p16.muscdn.com/img/tos-maliva-p-0068/3c816ae3779943c0a3c6d19da0c8204c_1574020710-tpiv-tiktok-shrL...	GET	200
DNS	13:05:14	http://p16.muscdn.com/img/tos-maliva-p-0068/0f94d0e67b6e4f0b9ed338670eca4e6b_1577566314-tpiv-tiktok-shrL...	GET	200
Own Traffic	13:05:14	https://p16.muscdn.com/img/musically-maliva-obj/e6252bedf8f919da07b42c203db009c-tpiv-tiktok-shrink:750:...	GET	200

```
Request Response Formatted Request
GET http://p16.muscdn.com/img/tos-maliva-p-0068/9d5bfecce020437a9e978b0e11f921a3_1579305427-tpiv-tiktok-shrink:248:330.webp?i1og=
HTTP/1.1
Host: p16.muscdn.com
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: TikTok/166800 CFNetwork/11.5.4 Darwin/16.7.0
Accept-Language: en-us
Accept: image/webp,image/*;q=0.8
```

FIGURE 10.15 Decrypted TikTok packet (pcap)

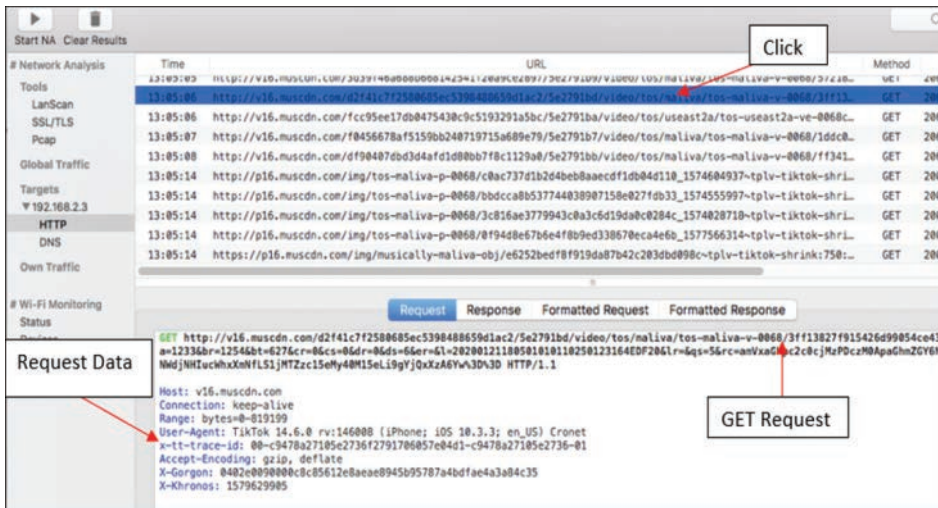


FIGURE 10.16 GET request data displayed

You may then click the **Response** tab to view the webpage or application response packet. Figure 10.17 displays a webpage response. Status code 200 means that it was successfully downloaded.

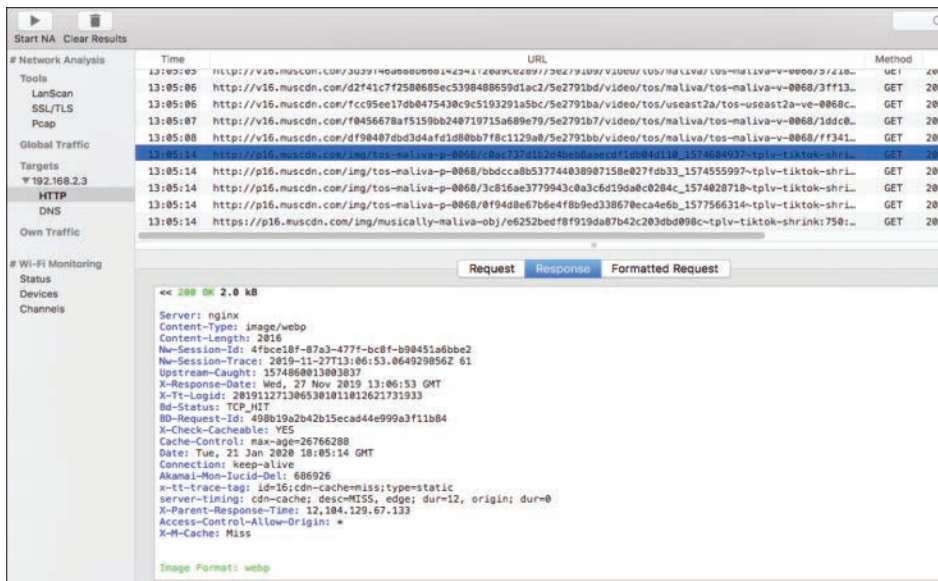


FIGURE 10.17 Response results

You can choose to export your packets so that they can be analyzed later. You can select to view your packet data in a text file or in a Word document. Figure 10.18 displays the option to export the packet data.

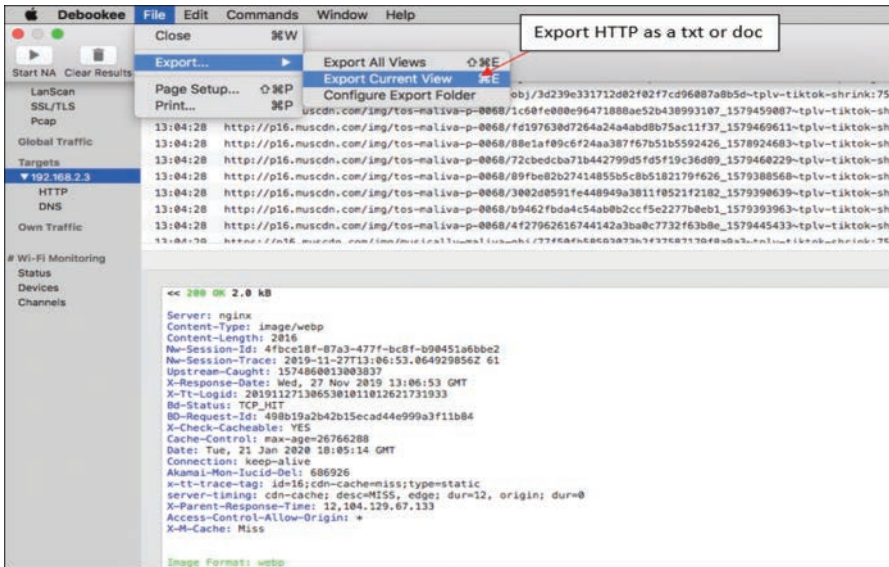


FIGURE 10.18 Data Export feature in Debookee

In Figure 10.19 and Figure 10.20 you can view the location and message data that was transmitted in plaintext while using the popular dating application Tinder. This data was observed while inspecting the entire packet in a text document.



FIGURE 10.19 Location, device, and user information from the Tinder app

```

"goingout": [],
"inbox": [],
"last_activity_date": "2019-03-21T15:28:35.757Z",
"liked_messages": [],
"lists": [],
"matches": [
  {
    "_id": "5c5cf250309d391100d25e8c5c5d9e488bb5ba1100d4d8d5",
    "is_new_message": true,
    "last_activity_date": "2019-03-21T15:28:35.757Z",
    "messages": [
      {
        "_id": "5c93ada33ae75815008049ae",
        "created_date": "2019-03-21T15:28:35.757Z",
        "from": "5c5cf250309d391100d25e8c",
        "match_id": "5c5cf250309d391100d25e8c5c5d9e488bb5ba1100d4d8d5",
        "message": "This is so confusing",
        "sent_date": "2019-03-21T15:28:35.757Z",
        "timestamp": 1553182115757,
        "to": "5c5d9e488bb5ba1100d4d8d5"
      }
    ]
  }
],
"places": {
  "has_new": false
}

```

Message sent from one Tinder user to another while intercepting with Debookee

FIGURE 10.20 Message from the Tinder App Displayed in Plaintext

The pcaps generated by Debookee can then be exported and analyzed using the Wireshark application. Wireshark can also perform data capture and is recommended for Windows users.

Dating Apps

There were 3.6 million applications (“apps”) on Google Play and 2.1 million iOS applications on Apple’s App Store in 2017, and a mere 8.5% of those apps were cross-platform, meaning that they were available for both iOS and Android. Adults in the United States are using mobile devices in ways that could not be imagined just 15 years ago. According to Pew Research Center’s report on mobile dating, 15% of adults (ages 18 and older), in the United States, have reported that they have used online dating sites or mobile dating apps. Dating site usage has nearly tripled for young adults (18 through 24) in just two years, from 10% to 27%. Therefore, it is important for investigators to understand the evidence available from mobile dating apps. Moreover, the prevalence of social engineering—using data derived from social media accounts—means that dating apps are a cause for concern in terms of organizational risk.

With the recent increase in online match-making connections, in a post-Snowden era where privacy has become a major concern, we might question whether dating applications are utilizing personal data ethically. In March 2018, a security flaw in the Grindr app disclosed user location data, which could have exposed app users to harassment; Grindr is a dating app, primarily used to connect gay men and unfortunately has facilitated numerous attacks against many gay men. Thus, understanding the available evidence from a dating app is extremely important because of the nature of the crimes being

committed, the links to social media, the personal information available, and the location and communication capabilities of these apps.

Tinder

As of 2018, Tinder had 57 million users worldwide. Millions of Tinder subscribers pay for a premium service: Tinder Plus or Tinder Gold. Tinder is used in 190 countries and supports 40 languages. Owned by Match Group, Inc., Tinder is a location-based, social media, application for dating. The app connects singles and allows them to “Swipe Right”, if they wish to connect with another individual, or they can “Swipe Left”, if they are not interested. The user can also “Swipe Up” (called a “super like”), which notifies the user that they have been “Super Liked”. The ability to passively block communication with someone, whom a user is not interested in, is what makes Tinder appealing for so many people.

Tinder gives the user the ability to chat with individuals who have both swiped right pseudo-anonymously. A user is not required to divulge his cellphone number, and a user can make his own judgment about how much personal information he wishes to share with another user when matched. Chats within the application are stored chronologically and can be deleted.

Tinder also offers a Web-based version of their service at gotinder.com and tinder.com (see Figure 10.21). The website gives users the ability to use Tinder’s services without a smartphone. The user simply logs in with their credentials. However, location services must be turned on, in the browser application, to use the Web version of the application.

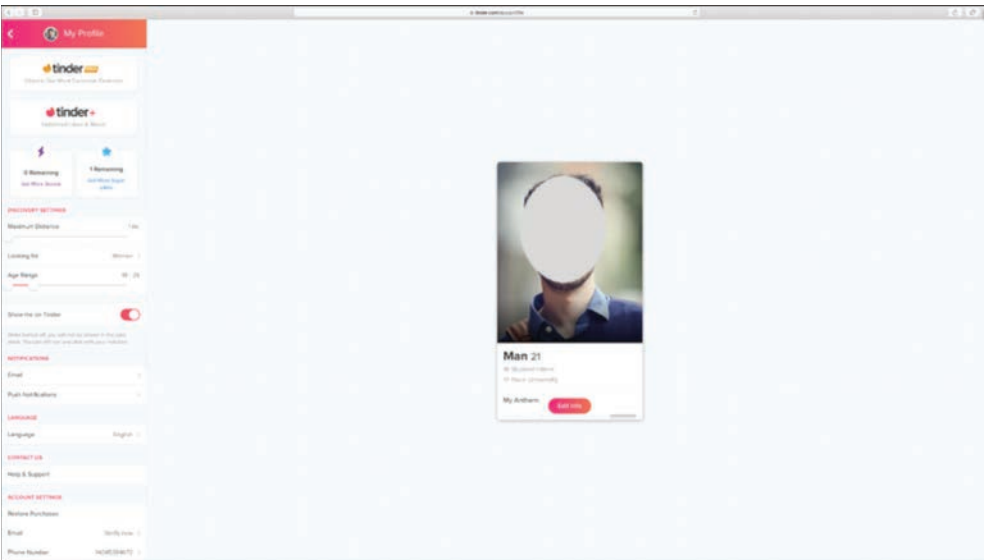


FIGURE 10.21 www.gotinder.com user profile

One of the most popular features of Tinder is the ability for users to synchronize their personal Instagram page with their Tinder profile (see Figure 10.22). This feature allows someone whom they have matched with (both parties swipe right) to have the ability to view the other user’s Instagram profile. This allows a user to visit a Tinder user’s Instagram profile, even if the Instagram account is set to private. Connecting social media accounts in this fashion is referred to as “deep-linking”.

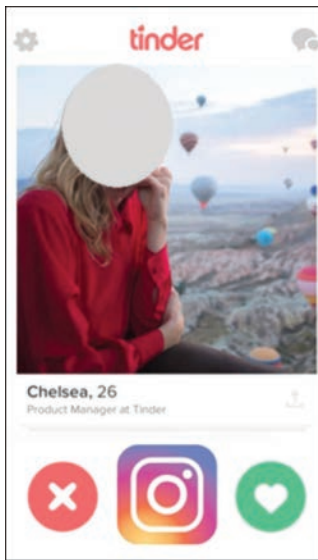


FIGURE 10.22 Tinder app linked to Instagram

A Spotify account can also be synchronized with a Tinder account, using deep-linking. This feature allows the users to share their personal playlists with individuals that they have matched with. A user can apply an “Anthem” to their profile, which can be the user’s favorite song.

Using Robtex (robtex.com), we can quickly map out the domains associated with Tinder, some of which are displayed in Figure 10.23.

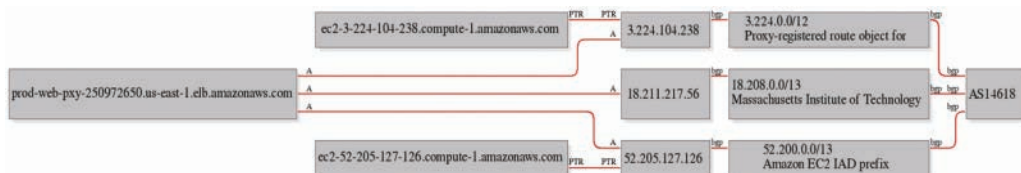


FIGURE 10.23 DNS data for gotinder.com (Source: Robtex.com)

Utilizing tools, like Robtex and traceroute, and whatismyipaddress.com, an investigator can determine where app user data is being stored and determining jurisdiction.

An analysis of Tinder’s DNS connections shows that the Tinder app connects a user’s profile with servers managed by Facebook, Leanplum, Appsflyer, DoubleClick, and many other companies. Using Debookee, it was possible to intercept Tinder messages, an example of which can be viewed in Figure 10.24. Figure 10.25 displays sample DNS connections associated with Tinder and captured with Debookee.

```

Host: api.gotinder.com
User-Agent: Tinder/10.5.0 (iPhone; iOS 10.3.3; Scale/2.00)
Accept: */*
Accept-Encoding: gzip, deflate
x-client-version: 10050013
platform: ios
Content-Type: application/json
os-version: 100000300003
Accept-Language: en-US;q=1
Connection: keep-alive
x-supported-image-formats: webp, jpeg
X-Auth-Token: 3e5e8de4-ab52-4b43-ba94-737cde82bfe8
Authorization: Token token="3e5e8de4-ab52-4b43-ba94-737cde82bfe8"
Content-Length: 34
app-version: 2665

{"message":"This is so confusing"}

```

FIGURE 10.24 Debookee HTTPS packet capture and decrypted chat message

```

11:28:27 api.gotinder.com 52.55.75.163 54.164.204.138
52.21.159.140 | 54.165.150.112 54.209.151.147 54.209.103.58
54.210.234.160 54.83.185.44
11:28:27 tinder-prod-pxy-1011891005.us-east-1.elb.amazonaws.com
52.55.75.163 54.164.204.138 52.21.159.140
54.165.150.112 54.209.151.147 54.209.103.58 54.210.234.160
54.83.185.44
11:28:31 etl.tindersparks.com 34.201.194.172 34.203.141.28
35.169.148.27 34.200.209.241 34.225.218.222 34.206.163.185
34.230.239.87 34.204.222.14
11:28:31 a8030d69c412411e989e80a34354f837-948153997.us-east-
1.elb.amazonaws.com 34.201.194.172 34.203.141.28 35.169.148.27
34.200.209.241 34.225.218.222 34.206.163.185 34.230.239.87
34.204.222.14
11:29:28 api.gotinder.com 34.203.153.190 52.202.189.239
34.225.27.3 3.93.229.43 52.0.63.52 52.20.184.210
34.232.174.172 34.202.104.117
11:30:29 api.gotinder.com 34.203.153.190 52.202.189.239
34.225.27.3 3.93.229.43 52.0.63.52 52.20.184.210
34.232.174.172 34.202.104.117
11:30:31 etl.tindersparks.com 34.201.194.172 3.85.248.212

```

FIGURE 10.25 DNS sample traffic captured with Debookee

Using BlackLight, a static analysis of the user data, contained in the Tinder SQLite database on an iPhone, reveals that the data is stored in plaintext. Interestingly, a private Instagram account could be viewed during this analysis. Moreover, that (private) Instagram account stored Instagram photos from other users without that user’s consent. User chat sessions, usernames, and Instagram data were all stored in plaintext on the iPhone test device. A URL can be found associated with each profile, which enables the user to access another user’s profile page—even if it is marked private.

An examination of the Tinder SQLite database also revealed the location of other Tinder users in close proximity, as shown in Figure 10.26.

ZDISTANCEMILES
1.0
1.0
6.0
1.0
1.0
1.0
6.0
3.0
7.0
5.0
1.0

FIGURE 10.26 ZDISTANCEMILES displays the distances to other users

It is also possible to obtain more precise information about users' locations in the vicinity, as shown in Figure 10.27.

```

"city": "New York",
"country": "US",
"county": "New York",
"dataProvider": "",
"deviceId": "F4CB8617-E5E2-4B7A-8C46-CAF8FA75BE0F",
"didSuperLike": false,
"gender": 0,
"hasUnsentMessage": false,
"heartbeatInMillis": 2000,
"language": "en-US",
"lastMessageFrom": "other",
"lat": 40.71,
"lon": -74.01,
"manu": "Apple",
"matchId":

```

FIGURE 10.27 Location data from the Tinder app

Grindr

While there are many mobile apps that provide corroborating evidence in an investigation, Grindr is an app that has been used to perpetrate some of the most heinous crimes. Therefore, it is an app that warrants special attention for investigators. Stephen Port, from East London, U.K., was called the Grindr Serial Killer after he was charged with murdering four men that he met on Grindr. There are literally hundreds, if not thousands of cases, where Grindr has been used, by criminals, to lure victims

and subsequently commit crimes, which include murder, assault, and robbery. The good news is that the Grindr app stores a wealth of information, in plaintext, which may help investigators and prosecutors.

Grindr was launched in 2009 and is the world's leading social networking application for gay, bisexual, trans and queer people. Grindr, unlike traditional dating apps, like Tinder and Bumble, is designed to find individuals in close proximity to the user. The smallest value for distance that Tinder/Bumble incorporates into their platform is one mile but Grindr will literally go to "zero feet away", and this is explicitly stated in the "About" section of their webpage. There is no "swipe left" or "dislike" and individuals are listed from closest to farthest away. There are no parameters to meet a certain type of user like with Tinder (age range, gender, etc.). If a user wants to engage with another user, they simply "Tap" that individual's profile, and they will be notified. The other user is then notified that they have been tapped. At this point, both users can immediately send an unlimited number of messages, which can be texts, images, and "GayMoji" stickers.

Popular dating applications, like Tinder and Bumble, require both users to explicitly indicate their willingness to engage with the other. However, Grindr does not require mutual consent to begin a chat session. There is a safeguard to protect from harassment, where the user can simply delete the "Tap" from a user they do not like, ending the message session. There are different types of "Taps" that give a visual representation of what the individual is looking for. There is a "Hi" icon tap for if the individual just wants to introduce himself or herself, or perhaps just chat. There is a "flame" icon tap for if the individual is interested in dating or sex. And finally, there is a "smiling devil Emoji" icon tap if the individual is looking for a "no strings attached" interaction. If the message is a text, then it will be previewed next to the user's profile. If it is a photo or video, it will have a small "Camera Icon" instead. A relatively new feature to the Grindr message function is "Read" receipts that will indicate whether the person a user messages has actually opened the message. Figure 10.28 shows the "Flame" tap and "Smiling Devil Tap" emojis.

Grindr has reached more than 196 countries with more than 3.6 million daily active users (2018). On average these users send 228 million messages and 20 million photos each day.

To date, there is no Web interface for Grindr, which supports user chat. However, the user can create a profile at www.grindr.com.

Grindr Evidence

Grindr does support deep-linking to social media services, which includes Facebook, Instagram, and Twitter. A feature of Grindr is the opportunity for a user to sync their personal Instagram page directly to their Grindr profile. This feature allows someone who has tapped on a user's Grindr profile to directly view the user's Instagram profile page. Grindr then gives the user the option to quickly switch directly to Instagram. This feature gives the user even more redundancy in deciding if the person they have matched with is someone they would still like to engage with. Both users still must go through the process of requesting to follow and allowing a follow through Instagram if the Instagram account is private. Like Instagram, a Facebook account can also be synced with a Grindr account, and it provides an easy one-click link directly to the Facebook profile on the Facebook app.

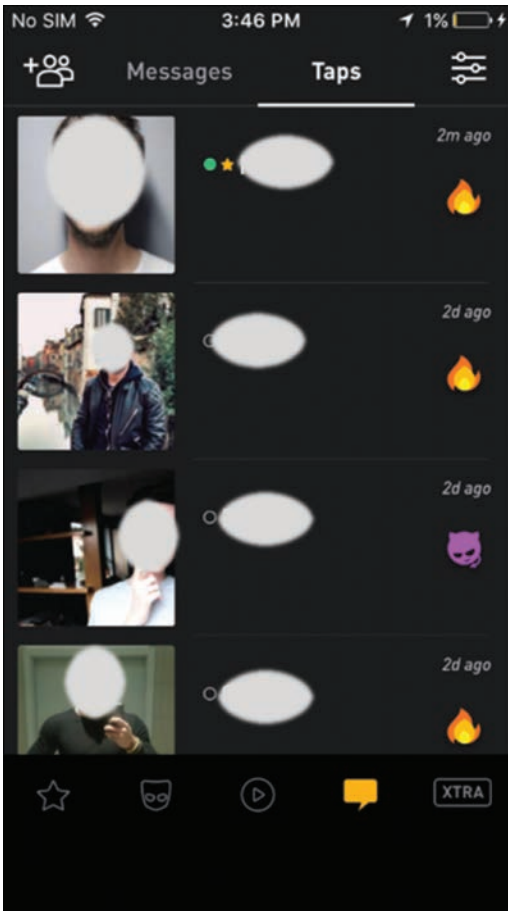


FIGURE 10.28 Grindr mobile user chat interface

Grindr appears to connect with a number of IP addresses, as displayed in Figure 10.29. A trace of these IP addresses goes back to San Francisco, California.

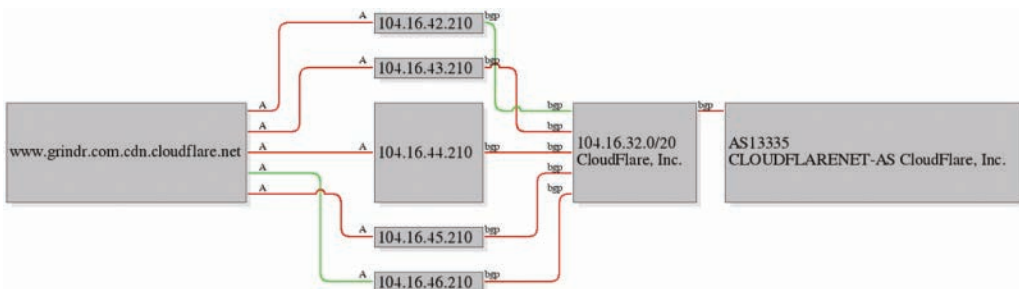


FIGURE 10.29 www.grindr.com.cdn.cloudflare.net DNS map (Source: Robtex.com)

Debookee could identify Grindr communication packets from iPhones, while they are being transmitted. The content is TLS/SSL encrypted. However, using the TLS decryption tool, offered by Debookee, it is possible to view a substantial amount of the DNS and HTTPS traffic, as shown in Figure 10.30. Messages are sent through *cdns.grindr.com* on port 443, using Amazon Web Services Inc. Although Grindr has made security updates to its platform since 2008, the third parties responsible for advertising, like Nexage, still pass sensitive PII, which includes exact location, sex, and age in plaintext, as shown in Figure 10.31. This means that anyone performing a man-in-the-middle attack could see that data.

```

GET
https://cdns.grindr.com/images/thumb/187x187/119ec148769261deac9753b958d1
05fa5c1b8047 HTTP/2.0

:authority: cdns.grindr.com:443
accept-language: en-us
accept: image/*;q=0.8
accept-encoding: gzip, deflate
user-agent: grindrx/5.5.2 (iPhone; iOS 10.3.3; Scale/2.00)

<< 403 213 B

date: Thu, 23 May 2019 16:27:28 GMT
content-type: application/xml
set-cookie: __cfduid=d368ff8b86152eab3a1603dif3c3a02511558628848;
expires=Fri, 22-May-20 16:27:28 GMT; path=/; domain=.grindr.com; HttpOnly
x-amz-request-id: 482245E3F27DAC58
x-amz-id-2:
GqyrEWlEYPmGGfVE6WQvQEa2y6UQMGPesksDfdflXVjE6DdGXfzdr2NbBPSCIK1iCYHwW/hja
GU=
cf-cache-status: HIT
expect-ct: max-age=604800, report-uri="https://report-
uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
vary: Accept-Encoding
server: cloudflare
cf-ray: 4db865c07cfb2214-EWR
content-encoding: gzip

```

FIGURE 10.30 Debookee HTTPS packet capture decryption

In a SQLite database, named *greventLog.sqlite*, you can find multiple latitude/longitude references stored in plaintext, as shown in Figure 10.32. Each message transaction is sent with updated location data. A latitude/longitude converter can then be used to find the address.

Messages in Grindr are unencrypted and are stored in plaintext. After viewing the data, a user has a unique identifier that is displayed in the “from” portion and in the “to” portion, which is a unique ID for the subject’s iPhone, as shown in Figure 10.33. After combing through *PersistenceStore.bin*, it is possible to see all message data generated between two devices. Incoming messages can also be retrieved in plaintext as shown in Figure 10.33.

```

cb348162a0e4e8aaafc96dd8259ba086_a9a6656256f74bb9979ed1c6e1cdda04,bae07051
d2a7499a9c394a84ff7028f6",
  "exclude_targeting_hash": "c8cce7cf889a841615a175ba5d9a59bd",
  "force_gdpr_applies": "0",
  "gdpr_applies": "0",
  "h": "1136",
  "id": "agltb3B1YilpbmNyDAsSBFNpdGUYorkhDA",
  "ll": "40.7106622970574,-74.00643135467496",
  "lla": "65",
  "llf": "446980",
  "llsdk": "1",
  "mr": "1",
  "nv": "5.4.1",
  "o": "p",
  "q": "app version:5.5.2",
  "request_id": "ddcb6bc67b114f729164e97a7f5978a0_00be2cd300d5de54",
  "rtc": "4",
  "sc": "2.0",
  "tar": "XObLdtR7RwsaIO9jOTZ2xgg9u2gcz0b4Wg8Yog",
  "udid": "mopub:788C666C-9774-4C3B-A9DD-D2535624C0E9",
  "user_data_c": "m_gender:m,m_age:20",
  "v": "8",
  "vv": "2",
  "w": "640",
  "z": "-0400"
}

```

FIGURE 10.31 Mopub banner ad including PII: Age, sex, and exact location

```

"carrier":null,"advertising_id":"00000000-0000-0000-0000-000000000000","cam
paign_id":null,"os_version":"iOS.10.3.3","notification_id":null,"timestamp"
:1554302044337.231,"notification_type":null,"latitude":"40.7105","longitude
":"-74.0065"}, {"name":"push_notification_clicked","timestamp":1554302044}, {"
params":{},"name":"inbox_screen_viewed","timestamp":1554302045}, {"params":{"
media_source":"None","campaign_name":"None","ad_set":"None"},"name":"link_
start","timestamp":1554302045}, {"params":{"network_status":"WIFI","distance_
setting_enabled":false,"push_enabled":"true","advertising_id":"00000000-00
00-0000-0000-000000000000","launch_type":"resume","launch_from_push":"true"
,"location_permission":"true"},"name":"app_opened","timestamp":1554302046},
{"params":{},"name":"tap_receive","timestamp":1554302048}, {"params":{},"nam
e":"tap_receive","timestamp":1554302048}, {"params":{},"name":"tap_receive",
"timestamp":1554302049}, {"params":{"source":"chat","type":"offline_photo",
time_passed_since_last_seen":null},"name":"chat_received","timestamp.Z.U [
.8A7B06F8-007D-4B90-B9EE-42475C281B4F[{"params":{"source":"inputbar_text_v
iew_focus"},"name":"chat_inputbar_item_click","timestamp":1554302454}, {"par

```

FIGURE 10.32 Latitude/longitude data from greventLog.sqlite

Uber

Uber is a service that enables drivers to act as flexible contractors and provide transportation services that compete with traditional taxi services. Consumers, using the Uber mobile app, can search for a car service in their area. The benefit to the consumer is that they are visually provided with the mapped location of Uber cars in their vicinity and are provided with an upfront quote for a specific journey (or “ride”). Uber operates in approximately 600 cities worldwide. In the past, Uber has received negative press about its geolocation tracking of users, which raised a number of concerns regarding its privacy policies and potentially invasive data collection practices. In April 2017, the *New York Times* published a story that documented a meeting, at Apple headquarters, in 2015, between Travis Kalanick, CEO of Uber, and Tim Cook, CEO of Apple. The article alleged that Mr. Cook scolded Mr. Kalanick for identifying and tagging iPhones after the Uber app had been uninstalled or the device had been wiped. Apparently, this type of user identity coding violated the Apple developer terms of service agreement.

An article in the *New York Times* detailed how Unroll.me, which purported to purge your device’s email inbox of annoying advertising messages, was used to spy on competitors. The article documented how Unroll.me would scan a user’s inbox, identify if there were service receipts, from competing companies like Lyft, and then sell that information to Lyft’s competitor—Uber.

Since the introduction of iOS 5, Apple has been limiting app developer access to the iPhone’s UDID (unique device identifier). A notice from Apple stated, “Starting May 1, the App Store will no longer accept new apps or app updates that access the UDID; please update your apps and servers to associate users with the Vendor or Advertising identifiers introduced in iOS 6.” Apple now prefers that app developers utilize the official Apple advertising platform to track app users. Based on Apple’s advertising and privacy policy, it appears that Apple does collect user data and then subsequently shares it with third parties. Nevertheless, developers can obtain extensive information about an app user through the integration of the UIDevice object. The UIDevice object can be used by an app developer to determine the assigned name of the device, device model and iOS version, orientation (orientation property) of the device, battery charge (batteryState property), and distance of the device to the user (proximity-State property). Moreover, developers can integrate code, during app development, for third-party analytics. These third-party companies include Localytics, mixpanel, UXCam, and Fabric. Companies like Apptopia provide app developers with extensive, nay invasive, analytics on competitor apps.

The use of the user UDID has not always been employed for nefarious purposes. However, the UDID was often utilized to identify if an app user was legitimate and could block a customer’s access if an account was compromised or potentially stolen. Fingerprinting is yet another methodology, used by third parties, to uniquely identify users, based on application configuration. Fingerprinting is best known for identifying online users based on user settings from their browser, which may include user cookies and browser plug-ins. The Electronic Frontier Foundation (EFF) created a project known as Panopticlick (panopticlick.eff.org) to raise awareness about how your browser is used by advertisers, and others, to identify and track you on the Web. The EFF announced that 84% of online users can be uniquely identified by their browser.

According to Uber’s user privacy statement, there are two categories of information collected about users: (a) Information You Provide to Us, which can include name, email, phone number, postal

address, profile picture, payment method, and (b) Information We Collect Through Your Use of Our Services, which can include location information, contacts, transactions, usage and preference, device information, call and SMS data, and log information. Of particular interest is the device information (hardware model, operating system and version, software and file names and versions, preferred language, unique device identifier, advertising identifiers, serial number, device motion information, and mobile network information). In terms of location information, Uber is not specific about the extent to which the user’s location is being tracked but states that they “may also collect the precise location of your device when the app is running in the foreground or background.” Uber provides more detailed information about the use of location services on its website under iOS App Permissions.

What is interesting is that during our installation of the Uber app, a dialog box appears and states that “Uber collects your location (i) when the app is open and (ii) from the time of the trip request through five minutes after the trip ends”, as displayed in Figure 10.21.

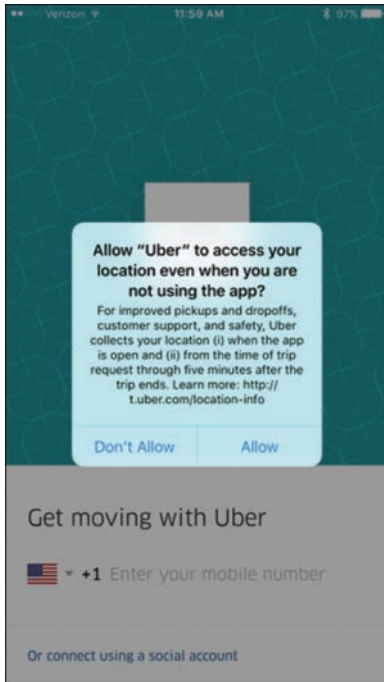


FIGURE 10.35 Uber dialog box during installation

Uber states in their FAQ that the reasoning behind this data collection is to “improve pickups, drop-offs, customer service, and to enhance safety.” However, users reported seeing the Uber app using location services weeks after the app was used and certainly beyond the stated 5 minutes. Uber responded to these reports blaming Apple’s iOS Maps extension that Uber uses to serve regional maps to their customers.

Perhaps unsurprisingly, Uber has invested heavily in data science to retain its competitive advantage, as evidenced by its aggressive recruitment of data scientists. We also know that Uber extensively uses a telematics pilot program, called Autohawk, to identify the location of its drivers and perform diagnostic testing on the vehicle to ensure passenger safety. In fact, Uber provides geolocation information, provided by its data visualization team, on its website at eng.uber.com/data-viz-intel. Uber integrates both Fabric and Localytics in its mobile app. Fabric provides companies, like Uber, with real-time information about the health of their app. These analytics include application crash analytics. Localytics provide location information.

As of November 2017, allegations abound about Uber's competitor spy programs. The *Waymo v. Uber* lawsuit appears to indicate that Uber may have been involved in illegal espionage. A letter, submitted as evidence in this lawsuit and penned by Richard Jacobs, former Uber security executive, details Uber's illegal practices of hiring actors to collect data and spy on their competitors. In the letter, Jacobs, who at the time had filed suit against Uber in the capacity of "whistleblower", detailed practices that would lead to the theft of trade secrets related to competitor fares and driver incentives. To settle, Uber paid Jacobs \$4.3 million at the time. His allegations have now been made public and have been used in a related case, *Waymo v. Uber*. In this case, a former employee allegedly sold trade secrets to Uber, prior to the company being acquired by Uber.

Communication Apps

Communication apps, such as WhatsApp, Signal, Viber, and Skype, are arguably more important than traditional cellphone or landline calls for numerous reasons. The first reason is that it is a lot easier to obtain content from these apps than to obtain a Title III Wiretap. Secondly, the content is so much richer than a traditional call or a text message. For example, consumers will share rich content, while reacting to the comments of others. In other words, you can find group chats that can link individuals and see emoticons and other reactions to messages that demonstrate personalization and behavior.

Skype

Law enforcement today understands that cellular communications generally account for a minority of smartphone communications. In fact, criminal gangs will often prefer using mobile communication apps over traditional cellular calls. Therefore, it is essential to have a good understanding of applications like Skype, Viber, enLegion, and WhatsApp.

Skype is a peer-to-peer (P2P) communication application that facilitates free video, voice, and instant messaging (IM) using a Wi-Fi connection. Skype also allows for file transfer to other Skype contacts and fee-based voice calls to landline phones and cellular phones using VoIP. Skype can be used with Mac computers, personal computers, tablets, smartphones, smart televisions, smart Blu-ray players, and game systems that include Xbox One and Sony's PS Vita PlayStation.

There are close to 300 million active monthly users worldwide. The company was purchased by Microsoft Corporation in 2011 for \$8.5 billion.

Skype Location

Location is important in terms of jurisdiction, when conducting an investigation. If the investigation is being conducted in the United States, then having a corporate location in the U.S. is helpful. However, even the presence of a server in the U.S. can enable law enforcement to subpoena that entity.

Skype is headquartered in Luxembourg but also has offices in London (U.K.), Palo Alto (U.S.A.) and Tallinn (Estonia), Prague (Czech Republic), Stockholm (Sweden), Moscow (Russia) and Singapore.

Skype Encryption

Instant messages (IM), between the Skype and chat service in the Cloud, are encrypted using TLS (transport-level security). IM between two Skype users are encrypted using AES (Advanced Encryption Standard). Voice messages are encrypted when sent to the recipient. However, when the voice message is downloaded and listened to, it is stored on the client's computer in an unencrypted way. Skype calls are also encrypted. When the user logs in, Skype will verify the user's public key using 1536 or 2048-bit RSA certificates.

Skype Evidence

The SQLite database file associated with Skype is `main.db`. The following files can be found within this SQLite database:

- DbMeta
- Contacts
- Videos
- SMSes
- CallMembers
- ChatMembers
- Alerts
- Conversations
- Participants
- VideoMessages
- LegacyMessages
- Calls
- Accounts
- Transfers

- Voicemails
- Chats
- Messages
- ContactGroups
- AppSchemaVersion
- MediaDocuments
- MessageAnnotations
- Translators
- tracker_journal

The Registry key associated with Skype is located here:

```
HKEY_CURRENT_USER\Software\Skype.
```

On a Windows PC, the file is located here:

```
%localappdata%\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\

```

On a Mac, the file is located here:

```
~/Library/Application Support/Skype/YourSkypeName/main.db
```

Table 10.1 and Table 10.2 display PLists associated with applications that may be of interest to investigators. More information about PLists can be found in Chapter 12, “Mac Forensics”.

TABLE 10.1 Application PLists

Application	SQLite File	PList
Facebook	Friends.sqlite	com.facebook.Facebook.plist
LinkedIn		com.linkedin.Linkedin.plist
Dropbox	Dropbox.sqlite	com.getdropbox.Dropbox.plist
Skype	main.db	com.skype.skype.plist
Amazon		com.amazon.Amazon.plist
eBay		com.ebay.iphone.plist
Google Maps	MapTiles.sqlitedb	
Tinder	Tinder2.sqlite	
WhatsApp	ChatStorage.sqlite	net.whatsapp.WhatsApp.plist

TABLE 10.2 Apple App .db Files

Apple App	SQLite File
Phone	AddressBook.sqlitedb
Calendar	Calendar.sqlitedb
Phone	Voicemail.db
Phone	Call_history.db
Messages	Sms.db
Safari	Safari/History.db
Maps	Maps/History.plist
Siri	ManagedObjects.SQLite

Summary

Mobile forensics has become extremely important for investigations because of the wealth of evidence available. The mobile apps found on a device are beneficial because of the fact that the data contained in the SQLite database is unencrypted for many mobile applications. Furthermore, deep-linking, which links one application to another application, enables an investigator to pull data from multiple sources while only examining one application. The data available during a static analysis can include contacts, chats, location data pictures, and other important evidence. As discussed, a SQLite database is a relational database that contains a series of tables. A static analysis is not limited to extracting evidence using forensics tools but also includes a review of the application manifest. The application manifest clearly identifies permissions associated with the application, which will help to guide the investigator to look for evidence related to those permissions. A dynamic analysis can assist an investigator in understanding potential third-party evidence, which is based on an app's connections to DNS servers when executed. Ultimately, these third-party companies can be subpoenaed for further evidence. A dynamic analysis can also determine the location of servers, associated with a mobile application, in terms of helping to identify jurisdiction. In this chapter, we spoke at length about mobile dating apps, which are important because of the extent of personal information available, primarily in the form of social media information. Dating apps are also important because we can also link people together. Grindr is particularly of interest to law enforcement because this dating app has actually been used to perpetrate crimes, especially hate crimes.

Key Terms

Android emulator: An application that simulates or runs the Android operating system in a virtual machine.

Android manifest file: A file that contains the application's package name, its functionality, permissions, hardware and software requirements for installation.

App ID: A two-part string that identifies a development team (Team ID) and an application (bundle ID).

bundle ID: A uniform-type identifier, which is comprised of alphanumeric characters, that uniquely identifies a specific app.

GET: An HTTP method used to request data from a specific resource, like a web server.

man-in-the-middle (MITM) attack: An attempt to intercept electronic communications between two computing devices with the intent to decipher encrypted messages.

pcap file: A wireless packet that contains user data and network data related to the sender and receiver of that data.

zero-day exploit: A security vulnerability that is a threat on the day that it is discovered because a software patch, to fix the exploit, does not yet exist.

Assessment

CLASSROOM DISCUSSIONS

1. Based on what you have learned in this chapter, from a security perspective, how can you determine if a mobile application is safe to use?
2. In what ways have mobile applications helped criminals and their criminal activities?
3. Under what circumstances is it legal to use wireless packet capture tools, like Wireshark or Debookee?

MULTIPLE-CHOICE QUESTIONS

1. An .apk file is associated with which of the following systems?
 - A. Android
 - B. iOS
 - C. Wireshark
 - D. Windows
2. Which of the following refers to a wireless packet that contains user data and network data related to the sender and receiver of that data?
 - A. pcap file
 - B. bundle ID
 - C. Android manifest file

FILL IN THE BLANKS

1. An Android _____ file contains the application's package name, its functionality, permissions, hardware and software requirements for installation.
2. An Android _____ is an application that simulates or runs the Android operating system in a virtual machine.
3. A(n) _____ file is a wireless packet that contains user data and network data related to the sender and receiver of that data.
4. A(n) _____ ID is a uniform-type identifier, which is comprised of alphanumeric characters, that uniquely identifies a specific app.
5. A(n) _____ ID is a two-part string that identifies a development team (Team ID) and an application (bundle ID).

6. A(n) _____-day exploit is a security vulnerability that is a threat on the day that it is discovered because a software patch, to fix the exploit, does not yet exist.
7. A man-in-the-_____ attack is an attempt to intercept electronic communications between two computing devices with the intent to decipher encrypted messages.
8. _____ is an HTTP method used to request data from a specific resource, like a web server.

PROJECTS

Write an Essay about a Mobile Application

Select a popular mobile app of your choice, which is not covered in this chapter and then perform a static and dynamic analysis on the app, using the analytics tools discussed in this chapter. Describe the value of the evidence that you find from (a) a digital forensics investigator perspective and (b) an organizational security and privacy viewpoint.

Symbols

\$USN_Journal, IOC, 355

Numbers

3GP wireless standard, 384–385, 416
3GP2 wireless standard, 385, 416
3GPP (3rd Generation Partnership Project), 384–385, 416
3GPP2 (3rd Generation Partnership Project 2), 385, 416
4G LTE Advanced, 383, 416
4G wireless standard, 383
5G wireless standard, 384, 573–575, 588
10-day notices, 130
800-byte files, physical layout of, 37
1980s, history of digital forensics, 15
1990s, history of digital forensics, 15–19
2000s, history of digital forensics, 20
***2600: The Hacker Quarterly*, 15**

A

ABA (American Bankers Association)
 ABA numbers, 165, 171
 Federal Reserve Bank reference list, 165
ABC fire extinguishers, 170
About This Mac feature (Apple), 527
Abrahams, Jared, photo forensics, case studies, 464

accelerometers, cellphones, 390, 417

access control lists, 51

AccessData, FTK training, 150

accessing

- computer forensics laboratories, 155
 - auditing access, 156
 - data access, 155–156
 - determining laboratory location, 157
 - physical security, 156
 - sign-in sheets, 156
- email, 6
- personal information
 - European Union (E.U.) access, 209
 - law enforcement access, 208–209
 - SIM cards, 388

accountants (forensic), 29

ACLU (American Civil Liberties Union), 177

ACPO (Association of Chief Police Officers), 303, 402

acronyms (IM), 198–199

action cameras, 583

actuator arms, 37–38

Adams, U.S. President John, 293

ADB (Android Debug Bridge), 398, 417

admissibility of evidence, 262, 305–306

- cellphone forensics, 393–396
- congressional legislation
 - CLOUD Act, 288
 - CALEA (47 U.S.C. § 1002), 284
 - Computer Fraud and Abuse Act (18 U.S.C. § 2511), 283
 - Corporate Espionage (18 U.S.C. § 1030(a)(1)), 283–284
 - Digital Millennium Copyright Act (DMCA) (17 U.S.C. § 1201), 286–287
 - Federal Wiretap Act (18 U.S.C. § 2511), 281–282
 - FISA-1978, 282–283

PROTECT Act, 286

USA PATRIOT Act (H.R. 3162), 14, 16–17, 268, 283, 284–286

Constitutional law, 262

criminal defense, 293–295

Daubert test, 289

depositions, 290, 307

Discovery phase, 290–291, 307

email, 6

Fifth Amendment (U.S. Constitution), 279–280

First Amendment (U.S. Constitution), 262–263

Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008), 265

Internet and, 263–265

Layschock et al v. Hermitage School District et al, 264–265

Miller v. California, 413 U.S. 15 (1973), 265

Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969), 263–264

forensics going wrong, 296

Fourth Amendment, 265–266

certiorari, 266, 306

exclusionary rule, 266, 307

fruit of the poisonous tree, 266, 278, 308

Katz v. United States, 389 U.S. 347 (1967), 266

O'Connor v. Ortega, 480 U.S. 709 (1987), 266

Olmstead v. United States, 277 U.S. 438 (1928), 266

search warrants, 266

warrantless searches, 268–271

Weeks v. United States, 232 U.S. 383 (1914), 266

FRE, 289–290

best evidence rule, 292–293, 306

depositions, 290, 307

- expert witnesses, 290–291
- FRCP, 290
- hearsay, 290, 291–292, 308
- Frye test, 288–289
- hearsay, 290, 291–292, 308
- photo forensics, 470
 - analog vs digital photography, 470–471
 - enhanced images, 471
 - FRE, 470
 - SWGDE, 470
- records of regularly conducted activity, 291
- rules for admissibility, 288–293
- Sixth Amendment (U.S. Constitution), 280–281
- ADN (Abbreviated Dialing Numbers), 386–387, 417**
- Adroit forensics, 153**
- ADS (Alternate Data Streams), 51**
- AES (Advanced Encryption Standard), 67**
- AFF (Advanced Forensics Format), 150, 170**
- AFF4 (Advanced Forensic File Format), 492, 531**
- Afifi, Asir, 273**
- AIM messages, 200**
- AirDrop, 531**
- AirPlay, 487, 531**
- AirPort Express, 488, 531**
- AirPort Extreme, 488, 531**
- AirPort Time Capsule, 488, 531**
- ALEAPP (Android Logs Events And Protobuf Parser), 399**
- Alerts (Google), searching for stolen property, 197**
- Alexa virtual assistant, 191, 578–579**
- algorithms, 28**
- Alito, Justice Samuel, 275**
- allocated storage space, 35–36**
- allocation blocks, 489–490, 531**
- AlphaBay, Dark Web investigations, 187–188**

- altered/fake images, 471**
- alternative volume headers, 489–490, 532**
- Amber Alert Bill, 16–17**
- AMBER alerts, 203–204, 216**
- AmCache, 357–358**
- amendments (U.S. Constitution)**
 - Fifth Amendment, 279–280
 - First Amendment, 262–263
 - Doninger v. Nieboff*, 527 F.3d 41 (2d Cir. 2008), 265
 - Internet and, 263–265
 - Laysbock et al v. Hermitage School District et al*, 264–265
 - Miller v. California*, 413 U.S. 15 (1973), 265
 - Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969), 263–264
 - Fourth Amendment, 265–266
 - certiorari, 266, 306
 - exclusionary rule, 266, 307
 - fruit of the poisonous tree, 266, 278, 308
 - Katz v. United States*, 389 U.S. 347 (1967), 266
 - O'Connor v. Ortega*, 480 U.S. 709 (1987), 266
 - Olmstead v. United States*, 277 U.S. 438 (1928), 266
 - search warrants, 266
 - warrantless searches, 268–271
 - Weeks v. United States*, 232 U.S. 383 (1914), 266
 - Sixth Amendment, 280–281, 306
- Amero, Julie, 296**
- analog vs digital photography, evidence admissibility, 470–471**
- analysis**
 - electronic media analyzed (reports), 240–241
 - Network Analyzer, 235

static analysis of applications (apps), SQLite database, 427–431

Twitter analytics, 204–205

Android OS, 200, 216, 391, 417

ADB, 398, 417

Android Auto, 391–392

Android manifest files, 429–430, 457

applications, 399–400

Brightest Flashlight, 430

Chip-Off, 395–396

EDL mode, 396–397, 417

emulators, 431, 457

evidence, 394–396

file systems, 392

forensics tools, 398

ISP, 396, 418

JTAG, 394–395, 418

partitions, 392–393

resources, 399

security, 396

USB debugging, 398, 420

anonymity, undercover investigations

Bluffmycall.com, 181–182

Spy Dialer, 182–183

ANPR (Automatic Number Plate Recognition), 585, 588

antennas/cell towers, locating, 375

anti-forensics, 365

anti-harrassment legislation, 557

antivirus software, 151

Antoine, Cheyenne Rose, 463

appellate courts

federal courts, 256–257

intermediate appellate courts, 257

state courts, 257

APFS (Apple File Systems), 490–491, 532

AFF4, 492, 531

APFS Free Queue, 492, 532

copy-on-write feature, 491, 532

data cloning, 491, 532

encryption, 491–492

keybags, 491–492, 533

metadata, 491

snapshots, 493, 534

space sharing, 492, 534

T2 security chip, 492

tmutil snapshot [enter], 493

API (Application Programming Interfaces), 204, 216

APK files, 430–431

APOLLO tool, 525–526, 583

App ID, 428, 457

appeals courts, 255–256

appendices/exhibits (reports), 241

Apple

About This Mac feature, 527

AirDrop, 531

AirPlay, 487, 531

AirPort Express, 488, 531

AirPort Extreme, 488, 531

AirPort Time Capsule, 488, 531

Apple Configurator, 526–527, 532

Apple ID, 510

Apple TV, 487–488

Apple Watch, 485, 581–583

Series 4, 485

Series 5, 486

Data Protection, 509, 532

deploying devices, 526–527

enterprise deployments, 526–527

Health application (app), 486–487, 530

history of, 480–481

iOS

Apple ID, 510

Data Protection, 509, 532

encryption, 509–510

- iOS 13, 508–509
 - media partitions, 508, 533
 - root partitions, 508, 534
 - security, 509–510
 - System Software Personalization, 508, 534
 - UDID, 509, 534
 - USB Restricted Mode, 510, 534
- iPad, 485, 487, 511, 530
- iPhone, 483–484, 511
 - APOLLO tool, 525–526
 - Apple Configurator, 526–527, 532
 - backups, 517, 522–523
 - batteries, 527
 - checkm8, 522
 - checkra1n, 522
 - DFU Mode, 512–513
 - enterprise deployments, 526–527
 - Face ID, 517, 532
 - Find My iPhone feature, 529
 - forensics, 511–526
 - iBeacon, 518, 533
 - iBoot, 513, 533
 - iCloud, 517–518, 533
 - imaging software, 512
 - iPhone 3G, 513
 - iPhone 3GS, 514
 - iPhone 4, 514
 - iPhone 5, 514
 - iPhone 5C, 514–515
 - iPhone 5S, 514
 - iPhone 6, 514–515
 - iPhone 6 Plus, 514–515
 - iPhone 11, 516
 - iPhone 11 Pro, 516
 - iPhone 11 Pro Max, 516
 - KTX Snapshots, 523–524
 - Location Services, 518–522, 533
 - Mail, 518
 - modes of operation, 512–513
 - Notes application (app), 523
 - original iPhone, 513
 - photos, 518, 523–524
 - Recovery Mode, 513, 534
 - Safari web browser, 518
 - Significant Locations, 521
 - SIM cards, 513
 - stolen iPhone case study, 529
 - Touch ID, 515–516, 534
 - user events, 525
- iPod, 482–483, 510–511
- iPod Touch, 482–483
- Mac, 481
 - About This Mac feature, 527
 - AFF4, 492, 531
 - APFS, 490–493, 532
 - App .db files, 456
 - Apple Configurator, 526–527, 532
 - Boot Camp, 92, 120, 489, 532
 - deleted files, 498
 - DMG images, 494, 498
 - email files, 501
 - enterprise deployments, 526–527
 - Epoch Converter, 497, 521
 - Epoch time, 496–497
 - forensics, 480, 492, 494–501, 527–528
 - Fusion Drives, 491, 494, 533
 - HFS, 489, 533
 - HFS+489–490
 - hibernation files, 501
 - initialization, 495, 533
 - IOReg Info, 495–496
 - journaling, 498
 - MAC addresses, finding, 337
 - MFS, 489, 533

PLists, 455, 499–501, 504–506

- PMAP Info, 495–496
- Quick Look, 494, 499, 534
- sleepimage files, 501, 534
- Spotlight feature, 494–495, 534
- SQLite database, 501, 505
- T2 security chip, 492
- Target Disk Mode, 506–507
- Terminal Window, 500

Mac mini, 481–482

macOS, 502

- Cache.db, 505
 - Catalina, 502–503
 - Cocoa, 499, 521, 522, 532
 - Cookies.plist, 505
 - deleted files, 498
 - Disk Utility, 503
 - displays (multiple), support for, 504
 - DMG images, 494, 498
 - Downloads.plist, 505
 - email files, 501
 - Epoch Converter, 497
 - Epoch time, 496–497
 - FileVault, 503, 532
 - Gatekeeper, 502–503, 533
 - hibernation files, 501
 - History.plist, 504–505
 - iCloud Keychain, 504, 533
 - initialization, 495, 533
 - IOReg Info, 495–496
 - journaling, 498
 - Keychain, 503
 - notifications, 504, 533
- Objective-C, 499, 533
- PLists, 455, 499–501
 - PMAP Info, 495–496

- Safari web browser, 504–506
- sleepimage files, 501, 534
- Spotlight feature, 494–495, 534
- SQLite database, 501
- tags, 504, 534
- Target Disk Mode, 506–507
- TopSites.plist, 506

Mac OS Extended. *See* HFS+

mobile devices, 507–510

System Software Personalization, 508, 534

USB Restricted Mode, 510, 534

Wi-Fi devices, 487–488

Apple Configurator, 526–527, 532**Application Layer (Layer 7), OSI model, 345, 365****applications (apps)**

- Android OS, 399–400, 417
- APK files, 430–431
- Brightest Flashlight, 430
- communication applications, 453–456
- Cop App application (app), 235
- dating applications, 441–442
 - Grindr application, 445–450
 - Tinder application, 442–445
- Digital Forensics Reference application (app), 235
- digital photography apps, 465–466
- documenting investigations, 234–236
- Facebook, photo forensics, 465
- Federal Rules of Evidence application (app), 236
- Flickr, 466
- FRCP application (app), 236
- Health (Apple), 486–487, 530
- Instagram, 466
- investigating, 457
 - communication applications, 453–456

- dating applications, 441–450
- Debookee, 433–441
- dynamic analysis, 431–433
- JSLint, 430–431
- pcap files, 431–432, 457
- rideshare applications, 450–453
- SQLite database, 427–431
- static analysis, 427–431
- wireless monitoring, 431–433
- Lock and Code application (app), 235
- Network Analyzer, 235
- Notes application (app), iPhone, 523
- PLists, 455, 499–501
- rideshare applications, 450–453
- Skype, 453–455
- SnapChat, 466
- static analysis of applications (apps), SQLite database, 427–431
- Strava application (app), 579–580
- System Status application (app), 235
- Uber application, 451–453
- Windows 8.1, 81
- wireless monitoring, 431–433
- zero-day exploits, 426, 457
- APT (Advanced Persistent Threats), 314–315, 349–350, 364, 365**
- archives (website), 189–190**
- Arizona v. Gant*, 2009, 271, 278**
- ARP (Address Resolution Protocol), 365**
 - OSI model, 342
 - requests, 321–322
- Articles of the Constitution, 254**
- ASCII (American Standard Code for Information Interchange), hexadecimal numbers**
 - hexadecimal to ASCII conversion, 44–45
 - hex editors, 46
- ASCLD (American Society of Crime Laboratory Directors), 127, 171**
- ASCLD/LAB, 127–129, 171**
- assistants (digital)**
 - Alexa, 191, 578–579
 - Cortana, 82–83
- Assisted GPS, 414, 417**
- ATM skimmers, 166–167, 171**
- attacks**
 - APT, 314–315
 - botnets, 577
 - cryptojacking, 577–578, 588
 - malware, VPN, 178
 - MITM attacks, 433, 457
 - network attacks, investigating, 357
 - AmCache, 357–358
 - EDR, 359
 - Kibana, 359
 - Log2Timeline, 359
 - RAM, 357
 - SANS SIFT workstation, 360–361
 - ShellBags, 358
 - ShimCache, 358
 - VSC, 358
 - Windows Registry, 361–363
- Trojan horses, 210, 218, 367**
 - zero-day exploits, 426, 457
 - Zeus, 210, 218
- attorneys, standby council, 564**
- attorneys**
 - defense attorneys, 293–294, 307
 - standby council, 564
- AuC (Authentication Center), 383, 417**
- auditing, laboratory access, 156**
- Auernheimer, Andrew “weev”283**
- authentication, AuC, 383, 417**
- Autopsy Video Triage, 213**
- AXIOM, 145, 212**

B**background searches, 177, 191–192**

- blogs, 202
- dynamic IP addresses, 207
- Google Groups, 201
- IM, 197–200
- IPv4 addresses, 206–207
- law enforcement access, 208–209
- locating suspects, 207
- metadata, 207
- personal information, 192–195
- personal interests, 195–196
- professional networks, 205–206
- public records, 206
- router forensics, 207–208
- social media, 196
- social networking websites, 202–205
- stolen property, 196–197
- usenet groups, 200–201
- user groups, 196

backup keybags, 492**backups**

- iPhone, 517, 522–523
- Windows 7
 - backing up to networks, 71–72
 - Backup and Restore Center, 69–71

bad sectors, 36**BALCO (Bay Areas Laboratory Company), 268****bash boards, 558, 563****Bates, James, 579****batteries**

- cellphones, 390
- iPhone, 527

Bayonet (Operation), Dark Web investigations, 187–188**BD (Blue-ray Discs), 115–116, 120****best evidence rule, 292–293, 306****BHO (Browser Help Objects), 365****Bill of Rights, The, 254, 262, 306****binary to decimal file conversion, 42****biographies (reports), 240****biometrics, Windows 7, 69****BIOS (Basic Input/Output System)**

- defined, 48
- viewing, 48–49

Bitcoin, 188, 216

- Bitcoin miners, 189, 216
- Bitcoin tumblers, 189, 216
- Bitcoin wallets, 188–189, 216
- blockchains, 189, 217
- identities, generating, 178

BitLocker, 10–11, 28**BitLocker To Go, 72****BitPim, 406–407****bit-stream imaging tools, 4, 28. See also forensic imaging software****BitTorrent, 191, 216****Blackbag Technologies**

- IOReg Info, 495–496
- PMAP Info, 495–496

BlackBerry 10, RIM OS, 400**BlackLight, 150****blockchains, 189, 217****blogs**

- background searches, 202
- Blog Search Engine, 202

Bluffmycall.com, 181–182**BMP files, 469, 474*****Bohach v. City of Reno*, 282****Boot Camp, 92, 120, 489, 532****boot process, 48–49****bootloaders, 396, 417****bootstrapping, 48****Boston Massacre, 293**

botnets, 577**BRB Publications, Inc.**206**Breivik, Anders Behring, 202****Brightest Flashlight, 430****brightness (images), 471, 474****Britton, Craig, 464****Brown, Governor Jerry, 278****browsers, 367**

Edge web browser, 82

viewing websites visited, 215

WebCacheV01.dat, 215, 218

InPrivate Browsing, Internet Explorer, 76–77

network forensics, 318–319

Safari, 504

Cache.db, 505

Cookies.plist, 505

Downloads.plist, 505

History.plist, 504–505

iPhone, 518

TopSites.plist, 506

webpage reviews, 504–505

for Windows, 506

Windows 7, 76–77

brute force attacks, 151, 171**BSC (Base Station Controllers), 377, 417****BTK killer, 117–118, 555–557, 563****BTS (Base Transceiver Stations), 373, 374–377, 417****budgets, computer forensics laboratories, 154****Bulger, James "Whitey"204****bundle ID, 428, 457****burden of proof, 260–261, 306****BWC (Body Wear Cameras), 584, 588****bytes**

800-byte files, physical layout of, 37

conversion table, 38–39

defined, 36

C**C2 (Command and Control), Intrusion Kill Chains, 352****CabinCr3w hactivist, 529****cabinets, computer forensics laboratories, 137****cabling**

FireWire cabling, 105–106, 121, 506–507, 532

SATA, 95–96, 97

ZIF cables, SATA, 96–97

Cache.db, 505**calculating IP subnet masks, 334–335****CALEA (Commission on Accreditation for Law Enforcement Agencies), 284****California v. Nottoli, 277–278****cameras (digital), 141–142. See also photo forensics**

BMP files, 469, 474

BWC, 584, 588

cellphones, 390–391

DCIM, 465, 474

digital photography apps, 465–466

DNG, 469, 474

DSCN, 465, 475

EXIF, 152, 466–467, 475

file types, overview of, 467–468

GIF files, 469, 475

JPEG files, 468, 475

PNG files, 469, 475

RAW files, 468–469, 475

TIFF files, 469, 475

capacity of hard disks, determining, 38**capturing online communications**

AXIOM, 212

cookies, 214

screen captures, 212–213

video, 213–214

websites visited, 215

Carpenter v. United States*, 278–279*CART (Computer Analysis and Response Teams), 15, 29****carving files, 145, 153, 171****case studies, 538, 563**

BTK killer, 555–557, 563

cyberbullying, 558–561

GPS tracking, 414

Las Vegas Massacre, 549–550

Mac forensics, 529–530

Major League Baseball (MLB), 561–562, 563

Moussaoui, Zacharias, 551–555, 563

photo forensics, 463, 471

Abrahams, Jared, 464

Antoine, Cheyenne Rose, 463

Britton, Craig, 464

Cole, Special Agent Jim, 463–464

extortion, 464

Gargol, Brittney, 463

INTERPOL, 471–473

IsAnybodyDown website, 464

Keating, Stephen, 463–464

NYPD Facial Recognition Unit, 473

Paul, Christopher Neil, 471–473

Wolf, Miss Teen USA Cassidy, 464

Silk Road, The, 538–549, 563

warrantless searches, 271

Catalina (macOS), 502–503**catalog files, 489–490, 532****Catalog ID, 489–490, 532****cause (probable), 267****CCPA (California Consumer Privacy Act),
criminal defense, 294****CCTV (Closed-Circuit Television), 8–9, 29****CD (Compact Discs), 113–114, 120**

lands, 113–114, 121

pits, 113–114, 121

sessions, 114, 115, 122

TOC, 114, 122

tracks, 36, 114, 122

**CDMA (Code Division Multiple Access), 385,
417****CDMA2000, 385, 417****CDR (Call Detail Records), 377–378, 412–413,
417****CD-ROM, frames, 114, 121****CD-RW (CD-Rewritable), 114–115****Celebrite UFED, 399, 408****cell sites, 374, 417****cellphones**

accelerometers, 390, 417

Android OS, 391, 417

ADB, 398, 417

Android Auto, 391–392

applications, 399–400

Chip-Off, 395–396

EDL mode, 396–397, 417

evidence, 394–396

file systems, 392

forensics tools, 398

ISP, 396, 418

JTAG, 394–395, 418

partitions, 392–393

resources, 399

security, 396

USB debugging, 398, 420

batteries, 390

cameras, 390–391

charging, 405–406

features, identifying, 404

forensics, 10, 372–374, 406, 416

3GP, 384–385, 416

3GP2, 385, 416

4G, 383

4G LTE Advanced, 383, 416

5G, 384, 588

- admissibility of evidence, 393–396
- ADN, 386–387, 417
- Android OS, 398, 417
- AuC, 383, 417
- BitPim, 406–407
- BTS, 373, 374–377, 417
- CDMA, 385, 417
- CDMA2000, 385, 417
- CDR, 377–378, 412–413, 417
- Celebrite UFED, 408
- containment devices, 403–404, 406
- documenting investigations, 415
- E3, 407–408
- EDGE, 384–385, 417
- EIR, 383, 417
- evidence, 388–389
- FCC-ID, 380, 404
- Fernico ZRT 3, 408–409
- flasher boxes, 409, 418
- FPLMN, 386–387, 418
- global satellite service providers, 410
- GPS devices, 413–414
- GrayKey, 406
- GRPS, 384–385
- GSM, 384, 418
- handsets, 406
- HLR, 382, 418
- iDEN, 385
- identifying cellphone features, 404
- IMEI, 378–379, 381–382, 418
- IMSI, 381, 418
- international numbering plans, 382–383
- ISPC, 382, 418
- ITU, 384
- legal considerations, 410–411
- LND, 386–387, 418
- logical versus physical examinations, 408
- manual examinations, 408–409
- MCC, 381, 418
- MEID, 379, 418
- MiFi, 383, 419
- MMS, 389, 419
- MNO, 383, 419
- MOBILedit! Forensic, 407
- MSIN, 381, 419
- MSISDN, 381, 419
- multiplexing, 385, 419
- MVNO, 383, 419
- NCIC, 209, 218, 411–412, 419
- Project-a-Phone, 408–409
- PUC, 388, 419
- PUK, 377–378, 388, 419
- RCS, 389, 419
- satellite communication services, 410
- SIM cards, 381–382, 385–388
- SMS, 388–389, 419
- SOP, 401–406
- subscribers, 377–378, 382–383, 420
- subsidy locks, 379, 420
- TAC, 378, 420
- TDMA, 384, 420
- TMSI, 382, 386–387, 420
- UMTS, 385, 420
- VLR, 382, 420
- W-CDMA, 384, 420, 384**
 - global satellite service providers, 410
 - handsets, 389
 - jammers, 155–156, 171
 - memory, 389–390
 - RIM OS, 400, 419
 - Samsung Galaxy, 393
 - Symbian OS, 400, 420
 - Windows 10 Mobile, 400, 420

cellular networks, 417

3GP, 384–385, 416
 3GP2, 385, 416
 4G, 383
 4G LTE Advanced, 383, 416
 5G, 384, 573–575, 588
 ADN, 386–387, 417
 AuC, 383, 417
 BSC, 377
 BTS, 373, 374–377, 417
 CDMA, 385, 417
 CDMA2000, 385, 417
 cell sites, 374, 417
 cell towers/antennas, locating, 375
 EDGE, 384–385, 417
 EIR, 383, 417
 FCC-ID, 380, 404
 FPLMN, 386–387, 418
 GRPS, 384–385
 GSM, 384, 418
 hard/soft handoffs, 377, 418, 420
 HLR, 382, 418
 ICCID, 381–382, 418
 iDEN, 385
 IMEI, 378–379, 381–382, 418
 IMSI, 381, 418
 international numbering plans, 382–383
 ISPC, 382, 418
 ITU, 384
 LND, 386–387, 418
 MCC, 381, 418
 MEID, 379, 418
 MiFi, 383, 419
 MMS, 389, 419
 MNO, 383, 419
 Mobile Stations, 378–383, 419
 MSC, 374, 419

MSIN, 381, 419
 MSISDN, 381, 419
 multiplexing, 385, 419
 MVNO, 383, 419
 PSTN, 374, 419
 PUC, 388, 419
 PUK, 377–378, 388, 419
 RCS, 389, 419
 SIM cards, 381–382, 385–388
 SMS, 388–389, 419
 subscribers, 377–378
 authentication, 382–383
 records, 377–378, 420
 subsidy locks, 379, 420
 TAC, 378, 420
 TDMA, 384, 420
 TMSI, 382, 386–387, 420
 UICC, 379, 420
 UMTS, 385, 420
 VLR, 382, 420

W-CDMA, 384, 420, 384**CERT (Computer Emergency Response Teams), 21****certifications, digital forensic training, 22–26****certiorari, 266, 306****CF (CompactFlash) cards, 110, 120****CF (Core Foundation), 499, 532****chain of custody, 2, 28, 229–230****chain of events, email, 5****charging cellphones, 405–406****check fraud**

Federal Reserve Bank reference list, 165
 GREP searches, 165–166

checkm8, 522**checkra1n, 522****children**

CIRCAMP, 18
 cyberbullying, 557

- anti-harassment legislation, 557
- defined, 558
- warning signs of, 557–558
- E.U. legal system, child pornography directives, 302–303
- ICAID, 18
- juvenile courts, 258, 308
- NCMEC
 - history of digital forensics, 15
 - photo forensics, 462–463
 - Project VIC, 463–464
 - United States v. Tank*, 292
- Chinese legal system, 304**
- Chip-Off, 395–396**
- CIRCAMP (COSPOL Internet Related Child Abuse Material Project), 18**
- City of Ontario v. Quon*, 282**
- City, State, Zip code expressions (GREP), 162**
- Civil law, 254, 306**
- civil trials versus criminal trials, 261–262**
- Civil War (U.S.), The, 253**
- claims court (small), 258**
- Class A networks, subnet masks, 332**
- Class B networks, subnet masks, 332**
- Class C networks, subnet masks, 332**
- "Clear Web"184**
- Clementi, Tyler, 559–560, 563**
- client computers, 9, 28**
- Clinton, U.S. President Bill, 183**
- cloning**
 - data, 491, 532
- devices, 98, 120, 137**
 - Disk Jockey PRO Forensic Edition, 98–101
 - ImageMASSter Solo IV Forensic, 101
 - Mac, 506–507
 - hard disk drives
 - PATA, 97
 - SATA, 97
 - SIM cards, 388
- CLOUD (Clarifying Lawful Overseas Use of Data) Act, 288**
- cloud computing**
 - iCloud, 517–518, 533
 - iCloud Keychain, 504, 533
- clusters, 36**
- CNN (Cable News Network), photo forensics case studies, 463–464**
- Cocoa, 499, 521, 522, 532**
- Codified law, 254, 306**
- COFEE (Computer Online Forensic Evidence Extractor), 72**
- CoinMarketCap, 188**
- Cole, Special Agent Jim, 463–464**
- colleges/universities, digital forensic training, 22**
- color balance (images), 471, 474**
- common law, 254, 306**
- communication**
 - applications (apps), 453–456
 - capturing online communications
 - AXIOM, 212
 - cookies, 214
 - screen captures, 212–213
 - video, 213–214
 - websites visited, 215
 - skills (digital forensics), 11
- CompactFlash, CF cards, 110, 120**
- comprehensive reports, creating, 238, 239**
 - biographies, 240
 - cover pages, 239
 - electronic media analyzed, 240–241
 - executive summaries, 239
 - exhibits/appendices, 241
 - findings of reports, 241
 - glossaries, 241–242
 - graphics, 238
 - investigative details connected to the case, 241
 - methodologies, 240, 246
 - proper/improper statements, 241

- purpose of investigation, 240
- structure of, 238–242

compression (file), 51**compromise (IOC), indicators of, 354, 357**

- \$USN_Journal, 355
- DLL files, 354
- email, 354
- event logs, 355–357
- MFT, 355
- MRU lists, 356
- ports, 355
- Prefetch files, 355
- PSExec, 356
- RAM, 357
- Registry keys, 354
- ServiceDLL, 354
- svc.host.eve, 354
- System32, 355
- UserAssist, 357

computer forensics

- imaging software, 143
- myths about, 3–4

computer forensics laboratories, 126, 170

- accessing, 155
 - auditing access, 156
 - data access, 155–156
 - determining laboratory location, 157
 - physical security, 156
 - sign-in sheets, 156
- antivirus software, 151

ASCLD/LAB, 127–129, 171

- budgets, 154
- cabinets, 137
- cloning devices, 137
- digital cameras, 141–142
- email preparation laboratories, 131
- energy requirements, 153

- ergonomics, 154

evidence

- acquisition laboratories, 131
- bags, 142
- labels, 143
- lockers, 136, 171
- extracting evidence from devices, 157
 - ATM skimmers, 166–167, 171
 - dd command, 157–158
 - EGREP, 160–161, 171
 - FGREP, 161–162, 171
 - GREP, 158–160, 162–166, 172
 - magstripe readers, 166–167, 172
 - parasites, 166, 172
 - skimmers, 166–168
 - steganalysis, 168, 172
 - steganography, 168–169, 172

- Faraday rooms, 135

- field kit storage units, 134–135

- flashlights, 141

- guidelines/standards, 127–130

- harvest drives, 140

- imaging software, 143, 144

- AXIOM, 145
- BlackLight, 150
- differences between tools, 143–144
- DriveSpy, 144
- E01 file format, 150, 171
- EnCase, 150
- EnScript, 150, 171
- F-Response, 145
- FTK, 7, 145, 149–150
- FTK Imager, 145, 146–149
- Guidance Software (opentext), 150
- ILook, 144
- Mac Marshal, 150
- Mobilyze, 145

- PALADIN, 145
- TSK, 144
- WinHex, 144
- X-Ways Forensics software, 144
- inventory control, 131
- ISO/IEC 17025.2017, 129
- laboratory information management systems, 131–132
- layout of, 132–133
- managing, 154–155
- password-cracking software, 151
- photo forensics, 152
 - Adroit forensics, 153
 - evidence, 152–153
 - EXIF data, 152
 - file formats, 152
 - metadata, 152
- private-sector computer forensics laboratories, 130
- safety, 153–154
- security, physical security, 156
- SIM card readers, 139–140
- SWDGE, 129–130, 172
- toolkits, 141
- VMware, 151
- web hosting, 132
- workbenches, 134, 172
- workstations, 133
- write-blockers, 137–139
- Computer Fraud and Abuse Act (18 U.S.C. § 2511), 283**
- computer hardware, 92–93**
 - CF cards, 110, 120
 - cloning devices, 98, 120
 - Disk Jockey PRO Forensic Edition, 98–101
 - ImageMASSter Solo IV Forensic, 101
 - disk controllers, 94, 121
 - FireWire cabling, 105–106, 121, 506–507, 532
 - flash drives, 106
 - hard disk drives, 93
 - cloning devices, 98–101
 - external hard drives, 107–108
 - HPA, 99, 100, 121
 - IDE, 93, 121
 - SATA, 95–97, 121
 - SCSI, 93–94, 122
 - write-blockers, 101, 107–108, 109, 112, 114, 122
 - memory
 - flash memory cards, 111–112
 - frames, CD-ROM, 114, 121
 - Memory Sticks, 110, 121
 - RAM, 103–104
 - removable memory, 105
 - xD Picture Cards, 111, 122
 - MMC, 108, 121
 - pits, CD, 113–114, 115, 121, 122
 - RAID, 104, 121
 - SD cards, 109–110, 112–113, 121
 - sessions, CD, 122
 - SSD, 101–103, 122
 - garbage collection, 102, 103, 121
 - TRIM function, 122
 - write-blockers, 109, 112
 - storage
 - BD, 115–116, 120
 - CD, 113–114, 120, 121
 - CD-RW, 114–115
 - DVD, 115, 120
 - floppy disks, 116–118, 121
 - magnetic tapes, 114–115, 121
 - zip disks, 118, 122
 - tracks (CD), 36, 114, 122
- computer science knowledge (digital forensics skills), 10–11**
- computer security, 29**

- computer toolkits, 141**
- computer worksheets, documenting investigations, 230–231**
- confidentiality (digital forensics skills), 12**
- Configurator (Apple), 526–527**
- Confrontation Clause, Sixth Amendment (U.S. Constitution), 281, 306**
- congressional legislation**
 - CLOUD Act, 288
 - CALEA, 284
 - Computer Fraud and Abuse Act (18 U.S.C. § 2511), 283
 - Corporate Espionage (18 U.S.C. § 1030(a)(1)), 283–284
 - DMCA, 286–287
 - Federal Wiretap Act (18 U.S.C. § 2511), 281–282
 - FISA-1978, 282–283
 - PROTECT Act, 286
 - USA PATRIOT Act (H.R. 3162), 14, 16–17, 268, 283, 284–286
- consent, Indian legal system, 304**
- Constitution (U.S.), 254**
 - Fifth Amendment, 279–280
 - First Amendment, 262–263
 - Doninger v. Niehoff*, 527 F.3d 41 (2d Cir. 2008), 265
 - Internet and, 263–265
 - Laysbock et al v. Hermitage School District et al*, 264–265
 - Miller v. California*, 413 U.S. 15 (1973), 265
 - Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969), 263–264
 - Fourth Amendment, 265–266
 - certiorari, 266, 306
 - exclusionary rule, 266, 307
 - fruit of the poisonous tree, 266, 278, 308
 - Katz v. United States*, 389 U.S. 347 (1967), 266
 - O'Connor v. Ortega*, 480 U.S. 709 (1987), 266
 - Olmstead v. United States*, 277 U.S. 438 (1928), 266
 - search warrants, 266
 - warrantless searches, 268–271
 - Weeks v. United States*, 232 U.S. 383 (1914), 266
 - Sixth Amendment, 280–281, 306
 - Supreme Court, The, 256
- Constitutional law, 254, 262, 306**
- consumer access/editing, Indian legal system, 304**
- Container Keybags, 491, 532**
- containment devices, cellphone forensics, 403–404, 406**
- contempt of court, 260, 307**
- Contents (reports), Table of, 239**
- continuous learning (digital forensics skills), 12**
- contrast (images), 471, 474**
- control of email, 5–6**
- control characters, hexadecimal to ASCII conversion, 45**
- converting files, 42**
 - binary to decimal, 42
 - hexadecimal numbers
 - conversion table, 42–43
 - hex converters, 45
 - hex editors, 45–46
 - hexadecimal to ASCII conversion, 44–45
 - hexadecimal to decimal file conversion, 43
 - hexadecimal to file type conversion, 47
- cookies, 217**
 - flash cookies, 214, 217
 - persistent cookies, 214, 218
 - session cookies, 214, 218
 - viewing, 214

Cookies.plist, 505

Cop App application (app), 235

copy-on-write feature (APFS), 491, 532

CoreStorage, 532

Corporate Espionage (18 U.S.C. § 1030(a)(1)), 283–284

Cortana, 82–83

counter-proliferation, 217

courts

appeals courts, 255–256

burden of proof, 260–261, 306

Court of Justice of the European Union, 297, 307

court orders, 272, 307

criminal trials versus civil trials, 261–262

cross-examination, 260–261, 307

deliberations, 261, 307

direct examination, 260–261, 307

federal courts

appellate courts, 256–257

jurisdiction, 256

Supreme Court, The, 256

U.S. District Courts, 257

felonies, 261, 307

juries, 260

contempt of court, 260, 307

foreperson, 260, 307

grand juries, 308

hung juries, 261, 308

indictments, 308

sequestration, 260, 308

voir dire, 260, 309

misdemeanors, 261, 308

opening statements, 260–261

procedural overview, 259–260

state courts, 257

appellate courts, 257

family courts, 258, 307

intermediate appellate courts, 257

juvenile courts, 258, 308

municipal courts, 258, 308

New York Trial Courts, 258–259

probate courts, 258, 309

small claims courts, 258, 309

traffic courts, 258, 309

trial courts of general jurisdiction, 258–259

trial courts of limited jurisdiction, 258

verdicts, 261

courts (U.S.), 254–255

admissibility of evidence, 262

Constitutional law, 262

First Amendment (U.S. Constitution), 262–265

Fourth Amendment (U.S. Constitution), 265–279

appeals courts, 255–256

burden of proof, 260–261, 306

court orders, 272, 307

criminal defense, 293

CCPA, 294

defense attorneys, 293–294, 307

NYS DFS Rule 23 NYCRR 500, 294–295

PIPEDA, 295

criminal trials versus civil trials, 261–262

cross-examination, 260–261, 307

deliberations, 261, 307

direct examination, 260–261, 307

en banc, 561, 563

federal courts

appellate courts, 256–257

jurisdiction, 256

Supreme Court, The, 256

U.S. District Courts, 257

felonies, 261, 307

judges, 255, 308

juries, 260

- contempt of court, 260, 307
- foreperson, 260, 307
- grand juries, 308
- hung juries, 261, 308
- indictments, 308
- sequestration, 260, 308
- voir dire, 260, 309
- misdemeanors, 261, 308**
 - motion in limine, 267, 308
 - Ninth U.S. Circuit Court of Appeal's, 268
 - opening statements, 260–261
 - pro se, 552
 - procedural overview, 259–260
 - standby council, 564
 - state courts, 257
 - appellate courts, 257
 - family courts, 258, 307
 - intermediate appellate courts, 257
 - juvenile courts, 258, 308
 - municipal courts, 258, 308
 - New York Trial Courts, 258–259
 - probate courts, 258, 309
 - small claims courts, 258, 309
 - traffic courts, 258, 309
 - trial courts of general jurisdiction, 258–259
 - trial courts of limited jurisdiction, 258
 - verdicts, 261
- cover pages (reports), 239**
- CPI (Counterfeit and Counter-proliferation Investigations), 211, 217**
- credit cards for sale, 210**
- Creepy, background searches**
 - geodata, 203
 - locating suspects, 207
- crime (online), 209**
 - CPI, 211
 - credit cards for sale, 210
 - cyberbullying, 211
 - electronic medical records, 210–211
 - identity theft, 210
 - social networking, 211–212
- crime scenes, documenting, 226**
 - CSI equipment, 228–229
 - evidence
 - evidence lists, 226–227
 - seizing, 227
 - on-scene examinations, 227–228
- criminal defense, 293**
 - CCPA, 294
 - defense attorneys, 293–294, 307
 - NYS DFS Rule 23 NYCRR 500, 294–295
 - PIPEDA, 295
- Criminal Procedure, Rules of, 270**
- criminal trials versus civil trials, 261–262**
- cropping images, 471, 474**
- cross-examination, 260–261, 307**
- cryptanalysis, 151, 171**
- crypto-currencies**
 - Bitcoin, 188, 216**
 - Bitcoin miners, 189, 216
 - Bitcoin tumblers, 189, 216
 - Bitcoin wallets, 188–189, 216
 - blockchains, 189, 217
 - identities, generating, 178
 - CoinMarketCap, 188
 - cryptojacking, 577–578, 588
 - Fiat currency, 188, 217
 - FinCEN, 188
 - history of digital forensics, 20
 - identities, generating, 178
 - IRS, 188
 - Linden dollars, 188
 - taxes, 188
 - Venmo, 189
 - Vicemo, 189

CSI (Crime Scene Investigation), equipment, 228–229

CTIN (Computer Technology Investigators Network), 21–22, 29

CUPS (Control and User Plane Separation), 574, 588

curtilage, 273, 307

custody, chain of, 2, 28, 229–230

C-V2X (Cellular Vehicle-to-Everything), 585, 588

Cyber Kill Chains, 350

C2, 352

delivery, 352

DLL side-loading, 353

exfiltration, 352

exploitation, 352

job postings, 351

persistence, 353

press releases, 351

reconnaissance, 350–352

remediation, 354

tech forums, 351

TTP, 352–353

weaponization, 352

YARA, 353

cyberbullying, 211, 557

anti-harrassment legislation, 557

bash boards, 558, 563

case studies, 558–561

defined, 558

doxing, 505, 560, 563

flaming, 558, 563

happy slapping, 558, 564

impersonation, 558, 564

online polls, 558, 564

outing, 558, 564

sexting, 558, 564

tricking, 558, 564

warning signs of, 557–558

Cyborg, 349

cylinders, 38

D

D2D (Device-to-Device), 574, 589

Dark Web investigations

AlphaBay, 187–188

Freenet, 186

I2P, 186

marketplaces, 186–188

Operation Bayonet, 187–188

OSINT Framework, 184

PlayPen, 187

Silk Road, The, 187, 188

Tails, 185, 218

Tor, 184–185, 218

data access, computer forensics laboratories, 155–156

data cloning, 491, 532

data forks (HFS), 489, 532

Data Link Escape, 45

Data Link Layer (Layer 2), OSI model, 342

data packets, 366

data privacy

E.U. legal system, 209, 298

Indian legal system, 304

Data Protection (Apple), 509, 532

data storage

BD, 115–116, 120

CD, 113–114, 120

lands, 113–114, 121

pits, 113–114, 121

sessions, 114, 115, 122

TOC, 114, 122

tracks, 36, 114, 122

CD-RW, 114–115

DVD, 115, 120

- floppy disks, 116–118, 121
- magnetic tapes, 114–115, 121
- wear-leveling, 122
- zip disks, 118
- databases (SQLite), 420, 501**
 - applications (apps), investigating, 427–431
 - Cache.db, 505
 - Mac forensics, 501
 - Tinder SQLite database, 427–429
- dates and times**
 - Epoch time, 496–497
 - HFS+490
- dating applications (apps), 441–442**
 - Grindr application, 445–450
 - Tinder application, 442–445
- Daubert v. Merrell Dow Pharmaceuticals*, 289**
- DCF (Design Rule for Camera File System), 465, 474**
- DCIM (Digital Camera IMages), 465, 474, 475**
- dd command, 119, 120, 157–158**
- DeadAim, 198, 217**
- Debookee, 433–441**
- debugging**
 - ADB, 398, 417
 - USB debugging, 398, 420
- decimal numbers**
 - binary to decimal file conversion, 42
 - hexadecimal to decimal file conversion, 43
- default gateways, 321, 365**
- defendants, 253, 307**
- defense (criminal), 293**
 - attorneys, 307
 - CCPA, 294
 - defense attorneys, 293–294, 307
 - NYS DFS Rule 23 NYCRR 500, 294–295
 - PIPEDA, 295
- defragmentation, Vista, 63–64**
- deleted files, macOS, 498**
- deliberations, 261, 307**
- delivery (Intrusion Kill Chains), 352**
- deploying Apple devices, 526–527**
- depositions, 290, 307**
- desktops, Windows 8.1, 80–81**
- DFU Mode, 512–513, 532**
- DHCP servers, 365**
 - ARP requests, 321–322
 - default gateways, 321
 - Event Viewer, 322
 - logs, 322–324
 - network forensics, 317–321
 - subnet masks, 321
 - viewing service activity, 322
- DHS (Department of Homeland Security)**
 - federal, state, local information exchange, 208
 - history of digital forensics, 16–17
- dictionary attacks, 151, 171**
- digital assistants**
 - Alexa, 191, 578–579
 - Cortana, 82–83
- digital cameras, 141–142. See also photo forensics**
 - BMP files, 469, 474
 - BWC, 584, 588
 - cellphones, 390–391
 - DCIM, 465, 474
 - digital photography apps, 465–466
 - DNG, 469, 474
 - DSCN, 465, 475
 - EXIF, 152, 466–467, 475
 - file types, overview of, 467–468
 - GIF files, 469, 475
 - JPEG files, 468, 475
 - PNG files, 469, 475
 - RAW files, 468–469, 475
 - TIFF files, 469, 475

digital evidence, 136**digital forensics, 29**

defined, 2

history of, 14–15, 27–28

1980s, 15

1990s, 15–19

2000s, 20

Amber Alert Bill, 16–17

DHS, 16–17

DoD, 16

ECTF, 16–17

encryption, 20

FARC, 16

FBI, 15

fusion centers, 18–19

INTERPOL, 17–18

IoT, 20

IRS, 16

NCMEC, 15

PC, 15

PROTECT Act, 16–17

RCFL, 18–19

Snowden, Edward, 20

USSS, 16–17

virtual currencies, 20

Digital Forensics Reference application (app),
235

importance of, 12–13

investigator skills

communication skills, 11

computer science knowledge, 10–11

confidentiality, 12

continuous learning, 12

legal expertise, 11

linguistic abilities, 12

programming, 12

job opportunities, 13–14

photo forensics, 464, 474

BMP files, 469, 474

brightness, 471, 474

case studies, 471–473

color balance, 471, 474

contrast, 471, 474

cropping images, 471, 474

DCF, 465, 474

DCIM, 465, 474

digital photography apps, 465–466

DNG, 469, 474

DSCN, 464, 475

enhanced images, 471

evidence admissibility, 470–473

EXIF, 152, 466–467, 475

EXIFextracter, 467

ExifTool, 467

Facebook, 465

fake/altered images, 471

file systems, 464–465

file types, overview of, 467–468

Flickr, 464

GIF files, 469, 475

Instagram, 466

JPEG files, 468, 475

linear filtering, 471, 475

megapixels, 467–468, 475

pixels, 467–468, 475

PNG files, 469, 475

raster-based graphics, 467–468

RAW files, 468–469, 475

SnapChat, 466

SWGIT, 471, 475

TIFF files, 469, 475

tumbcache.db, 469

vector graphics, 468, 475

professional certifications, 22–26

recovered evidence, types of, 5

- cellphones, 10
- email, 5–6
- images, 7–8
- IoT, 10
- video, 8–9
- training/education, 21
 - colleges/universities, 22
 - high schools, 22
 - law enforcement, 21–22
- digital surveillance, search warrants, 272–273**
- digital vs analog photography, evidence admissibility, 470–471**
- direct examination, 260–261, 307**
- Discord, 200**
- discovery periods, 132, 171**
- Discovery phase (trials), 290–291, 307**
- disk controllers, 94, 121**
- disk geometry, 38**
- disk images, 97, 121**
- Disk Jockey PRO Forensic Edition, 98–101**
- Disk Signatures, 49**
- disk storage**
 - BD, 115–116, 120
 - CD, 113–114, 120
 - lands, 113–114, 121
 - pits, 113–114, 121
 - sessions, 114, 115, 122
 - TOC, 114, 122
 - tracks, 36, 114, 122
 - CD-RW, 114–115
 - DVD, 115, 120
 - floppy disks, 116–118, 121
 - zip disks, 118, 122
- Disk Utility (macOS), 503**
- Disney, stolen iPhone case study, 529**
- displays (multiple), macOS support, 504**
- disposable email services, 179–181**
- District Courts (U.S.), 257**
- DLL (Dynamic Link-Layer), 365**
 - IOC, 354–354
 - ServiceDLL, 354
 - side-loading (Intrusion Kill Chains), 353
- DMCA (Digital Millennium Copyright Act), 286–287**
- DMG images, 494, 498, 532**
- DNG (Digital Negatives), 469, 474**
- DNS (Domain Name System), 365**
 - network forensics, 326–327
 - protocol, 328
- documenting investigations, 224, 245**
 - cellphone forensics, 415
 - Chain of Custody forms, 229–230
 - Cop App application (app), 235
 - crime scenes, 226
 - evidence lists, 226–227
 - on-scene examinations, 227–228
 - seizing evidence, 227
 - CSI equipment, 228–229
 - Digital Forensics Reference application (app), 235
 - expert witnesses, 242, 246
 - goals of, 242
 - preparing for trial, 243–244
 - role of, 242
 - tips for prosecution, 244
 - Federal Rules of Evidence application (app), 236
 - FragView, 234
 - FRCP application (app), 236
 - hard disk drive worksheets, 232
 - ISP, obtaining evidence from, 224–225
 - lay witnesses, 243, 246
 - Lock and Code application (app), 235
 - Network Analyzer, 235
 - photos, 231
 - preservation orders, 225, 246

reports, 238, 239
 biographies, 240
 cover pages, 239
 DST, 236–237, 246
 electronic media analyzed, 240–241
 executive summaries, 239
 exhibits/appendices, 241
 findings of reports, 241
 forensic tools, 236
 glossaries, 241–242
 graphics, 238
 investigative details connected to the case, 241
 methodologies, 240, 246
 proper/improper statements, 241
 purpose of investigation, 240
 structure of, 238–242
 time zones, 236–238
 server worksheets, 233–234
 System Status application (app), 235
 tagged evidence, 229
 tools/applications, 234–236

DoD (Department of Defense), history of digital forensics, 16

dogs, vehicle forensics, 586–587

DOJ (U.S.), warrantless searches, 268

Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008), 265

Downloads.plist, 505

doxing, 560, 563

DriveSpy, 144

drones, 584

DSCN (Digital Still Capture Nikon), 465, 475

DST (Daylight Savings Time), documenting investigations, 236–237, 246

Dual Shot, 393

DVD (Digital Video Disks), 115, 120

dynamic analysis, applications (apps), 431–433

dynamic IP addresses, 207, 217

E

E01 forensic disk image file format, 150, 171

E3, 407–408

ECTF (Electronic Crimes Task Forces), 16–17, 29

EDGE (Enhanced Data Rates for GSM Evolution), 384–385, 417

Edge web browser, 82

WebCacheV01.dat, 215, 218

websites visited, viewing, 215

eDiscovery, 13, 29, 130, 171

EDL mode, 396–397, 417

EDR (Endpoint Detection and Response), 359

education/training, 21

colleges/universities, 22

high schools, 22

law enforcement, 21–22

professional certifications, 22–26

EGREP (Extended Global Regular Expressions Print), 160–161, 171

EIR (Equipment Identity Register), 383, 417

Electronic Crime Scene Investigation: A Guide for First Responders, 226–227

electronic media analyzed (reports), 240–241

electronic medical records, 210–211

email

accounts, generating, 179

GuerillaMail, 179–180

mail expire, 180

Mailinator, 181

as digital evidence, 5

accessibility, 6

admissibility, 6

- chain of events, 5
- control, 5–6
- intent, 5–6
- ownership, 5–6
- prevalence, 6
- tampering with evidence, 6
- disposable email services, 179–181
- email preparation laboratories, 131
- identities, generating, 178
- IOC, 354
- Mac forensics, 501
- macOS email files, 501
- Mail, iPhone, 518
- MIME, 326, 365
- network forensics, 325–326
- SMTP servers, 325–326
- United States v. Ziegler*, 267
- Email Address expressions (GREP), 162**
- emulators, Android OS, 431, 457**
- en banc, 561, 563**
- EnCase, 150**
- encryption, 9, 29**
 - AES, 67
 - APFS, 491–492
 - FileVault (macOS), 503, 532
 - history of digital forensics, 20
 - iOS, 509–510
 - KEK, 491, 533
 - OpenPGP, network forensics, 330
 - PGP encryption
 - network forensics, 329–330
 - OpenPGP, 330
 - VEK, 491, 534
- End of Sector Markers, 49**
- endpoints, EDR, 359**
- energy requirements, computer forensics laboratories, 153**
- Enhanced 911, 414, 417**
- enhanced images, admissibility of evidence, 471**
- EnScript, 150, 171**
- Epoch Converter, 497, 521**
- Epoch time, 496–497**
- ergonomics, computer forensics laboratories, 154**
- eSATA connectors, 96, 121**
- escrow keybags, 492**
- ESI (Electronically Stored Information), 130, 171**
- ESN (Electronic Serial Numbers), 417**
- E.U. (European Union). See also U.K.**
 - data privacy, 209, 298
 - European Commission, 307
 - legal system, 296–297
 - ACPO, 303
 - child pornography directives, 302–303
 - Court of Justice of the European Union, 297, 307
 - European Commission, 297
 - European law, origins of, 297
 - European law, structure of, 297–303
 - Europol, 303
 - Facebook, 302
 - GDPR, 298–301
 - intellectual property, 302
 - Investigative Powers Act of 2016, 302
 - Judex, 297, 308
 - legislatures, 297
 - OLAF, 303
 - UK Modern Slavery Act, 301
 - Legislature, 307
- Europol, 303**
- event logs, IOC, 355–357**
- Event Viewer, 65–66, 76, 322**
- events (email), chain of, 5**
- evidence**

- admissibility, email, 6
- admissibility of, 262, 305–306
 - best evidence rule, 292–293, 306
 - cellphone forensics, 393–396
 - certiorari, 266, 306
 - congressional legislation, 281–288
 - Constitutional law, 262
 - criminal defense, 293–295
 - Daubert test*, 289
 - depositions, 290, 307
 - Discovery phase, 290–291, 307
 - exclusionary rule, 266, 307
 - expert witnesses, 290–291
 - Fifth Amendment (U.S. Constitution), 279–280
 - First Amendment (U.S. Constitution), 262–265
 - forensics going wrong, 296
 - Fourth Amendment (U.S. Constitution), 265–279
 - FRCP, 290
 - FRE, 289–293
 - fruit of the poisonous tree, 266, 308
 - Frye test, 288–289
 - hearsay, 290, 291–292, 308
 - Katz v. United States*, 389 U.S. 347 (1967), 266
 - O'Connor v. Ortega*, 480 U.S. 709 (1987), 266
 - Olmstead v. United States*, 277 U.S. 438 (1928), 266
 - records of regularly conducted activity, 291
 - rules for admissibility, 288–293
 - search warrants, 266
 - Sixth Amendment (U.S. Constitution), 280–281
 - warrantless searches, 268–271
 - Weeks v. United States*, 232 U.S. 383 (1914), 266
 - best evidence rule, 292–293, 306
 - cellphone forensics, 388
 - MMS, 389, 419
 - RCS, 389, 419
 - SMS, 388–389, 419
 - Discovery phase, 290–291, 307
 - documenting, 229
 - Chain of Custody forms, 229–230
 - Cop App application (app), 235
 - Digital Forensics Reference application (app), 235
 - evidence lists, 226–227
 - Federal Rules of Evidence application (app), 236
 - FragView, 234
 - FRCP application (app), 236
 - hard disk drive worksheets, 232
 - Lock and Code application (app), 235
 - Network Analyzer, 235
 - photos, 231
 - server worksheets, 233–234
 - System Status application (app), 235
 - tools/apps, 234–236
 - evidence acquisition laboratories, 131
 - evidence bags, 142
 - evidence labels, 143
 - evidence lockers, 136, 171
 - exculpatory evidence, 2, 29
 - extracting from devices, 157
 - ATM skimmers, 166–167, 171
 - dd command, 157–158
 - EGREP, 160–161, 171
 - FGREP, 161–162, 171
 - GREP, 158–160, 162–166, 172
 - magstripe readers, 166–167, 172
 - parasites, 166, 172
 - skimmers, 166–168

- steganalysis, 168, 172
- steganography, 168–169, 172
- Federal Rules of Evidence
 - application (app), 236
 - expert witnesses, 242
- firewall evidence, 340
- FRE, 289–290, 470
 - best evidence rule, 292–293, 306
 - depositions, 290, 307
 - expert witnesses, 290–291
 - FRCP, 290
 - hearsay, 290, 291–292, 308
- gathering, Windows 8.1, 81–82
- hearsay, 290, 291–292, 308
- IM, 199–200
- inculpatory evidence, 2, 29
- ISP, obtaining evidence from, 224–225
- photo forensics, 152–153, 231
 - admissibility, 470–473
 - analog vs digital photography, 470–471
 - enhanced images, 471
 - fake/altered images, 471
- preservation orders, 225, 246
- seizing, 227
- spoilation of, 12, 30
- SWGDE, 470
- tagged evidence, documenting, 229
- Transfer of Evidence, 4
- tampering with, 6, 30
- website evidence, 189
 - website archives, 189–190
 - website statistics, 190–191
- exclusionary rule, 266, 307**
- exculpatory evidence, 2, 29**
- executive summaries (reports), 239**
- exFAT, 464**
- exfiltration (Intrusion Kill Chains), 352**

- exhibits/appendices (reports), 241**
- EXIF (Exchangeable Image File Format), 152, 466–467, 475**
- EXIFextracter, 467**
- ExifTool, 467**
- exigent circumstances, 268, 307**
- expert witnesses, 242, 246, 290–291**
 - goals of, 242
 - prosecution, tip for, 244
 - role of, 242
 - trial, preparing for, 243–244
- exploitation (Intrusion Kill Chains), 352**
- external hard drives, 107–108**
- extortion, photo forensics case studies, 464**
- extracting evidence from devices, 157**
 - ATM skimmers, 166–167, 171
 - dd command, 157–158
 - EGREP, 160–161, 171
 - FGREP, 161–162, 171
 - GREP, 158–160, 172
 - check fraud searches, 165–166
 - expressions, 162–163
 - financial fraud searches, 163–165
 - magstripe readers, 166–167, 172
 - parasites, 166, 172
 - skimmers, 166–168
 - steganalysis, 168, 172
 - steganography, 168–169, 172

F

- Face ID (iPhone), 517, 532**

Facebook

- AMBER alerts, 203–204
- background searches, 203–204
- E.U. legal system, 302
- photo forensics, 461–462, 465

- Face.com, 465**

facial recognition, 584

Face ID (iPhone), 517, 532

NYPD Facial Recognition Unit, 473

Fake Name Generator, 179**fake/altered images, 471****family courts, 258, 307****Faraday boxes, 403–404, 406****Faraday rooms, 135****FARC, history of digital forensics, 17–18****Farid, Hany, 471****FAT (File Allocation Tables), 464**

defined, 50

FAT12, 50

FAT16, 50

FAT32, 50

FAT64, 50

FATX, 50

fault tolerance, 104, 121**FBI (Federal Bureau of Investigation)**

CART, 15

history of digital forensics, 15

Ten Most Wanted list, 460

FCC (Federal Communications Commission)

cellular telephone jammers, 155–156

FCC-ID, 380, 404, 418

federal, state, local information exchange, 208–209**federal courts**

appellate courts, 256–257

jurisdiction, 256

Supreme Court, The, 256

U.S. District Courts, 257

Federal Reserve Bank reference list, check fraud, 165**Federal Wiretap Act (18 U.S.C. § 2511), 281–282*****Federalist Papers*, 287****felonies, 261, 307****Fernico ZRT 3, 408–409****FGREP (Fast Global Regular Expressions Print), 161–162, 171****Fiat currency, 188, 217****field kit storage units, 134–135****Fifth Amendment (U.S. Constitution), 279–280****file systems**

Android OS, 392

APFS, 490–491

AFF4, 492, 531

APFS Free Queue, 492, 532

copy-on-write feature, 491, 532

data cloning, 491, 532

encryption, 491–492

keybags, 491–492, 533

metadata, 491

snapshots, 493, 534

space sharing, 492, 534

T2 security chip, 492

tutil snapshot [enter], 493

Fusion Drives, 491, 494, 533

HFS, 489, 533

HFS+489–490

MFS, 489, 533

NTFS

defined, 50, 51–52

FTK Imager, 53–56

MFT, 52

system files, 53

photo forensics, 464–465

SIM cards, 386–387

Windows

defined, 49

FAT, 50, 464

FAT12, 50

FAT16, 50

FAT32, 50

FAT64, 50

- FATX, 50
- feature comparisons table, 52
- NTFS, 50, 51–52, 53–56
- Prefetch files, 57, 355, 366
- ShellBags, 58
- ShimCache, 58–59
- Superfetch files, 58
- Windows Registry, 59–62

files

- APFS file metadata, 491
- Cache.db, 505
- carving, 145, 153, 171
- catalog files, 489–490, 532
- compression, 51
- conversion, 42
 - binary to decimal, 42
 - conversion table, 42–43
 - hex converters, 45
 - hex editors, 45–46
 - hexadecimal to ASCII conversion, 44–45
 - hexadecimal to decimal file conversion, 43
 - hexadecimal to file type conversion, 47
- deleted files, macOS, 498
- DMG images, 494, 498
- email files, macOS, 501
- formats, photo forensics, 152
- grouping, Windows 7, 78
- hosts files, 327–328, 365
- Linux, network forensics, 317–318
- macOS
 - email files, 501
 - hibernation files, 501
 - sleepimage files, 501, 534
- metadata, 29
 - images, 7
 - Vista, 67
- PList files, 455, 499–501
 - Cookies.plist, 505

- Downloads.plist, 505
- History.plist, 504–505
- TopSites.plist, 506
- Prefetch files, 57, 355, 366
- slack, 37, 46
- storage
 - 800-byte files, physical layout of, 37
 - bad sectors, 36
 - bytes, 36, 38–39
 - clusters, 36
 - file slack, 37, 46
 - logical file size, 36
 - physical file size, 36
 - sectors, 36
 - tracks (CD), 36, 114, 122
- Superfetch files, 58
- types, hexadecimal number conversions to, 47

FileVault (macOS), 503, 532

financial fraud

- GREP searches, 163–165
- IIN matrix, 163
- MII charts, 163

FinCEN (Financial Crimes Enforcement Unit), 188

Find My iPhone feature (Apple), 529

finding

- MAC addresses, 336–337
 - iPhone, 337
 - Mac (Apple), 337
 - PC, 336
- personal information, 192–195
- subnet masks, 335

findings of reports, documenting investigations, 241

fire extinguishers (ABC), 170

firewalls, 365

- evidence, 340
- network forensics, 339–340

NGFW, 339–340
 proxy firewalls, 339–340
 stateful inspection firewalls, 339–340
 stateless firewalls, 339–340
 UTM, 339–340

FireWire cabling, 105–106, 121, 506–507, 532

firmware, 151, 171, 512–513

First Amendment (U.S. Constitution), 262–263
Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008), 265
 Internet and, 263–265
Laysbuck et al v. Hermitage School District et al, 264–265
Miller v. California, 413 U.S. 15 (1973), 265
Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969), 263–264

FISA-1978 (Foreign Intelligence Surveillance Act-1978), 282–283

fitness trackers, 579–580

Five Eyes, 20, 29

flaming, 558, 563

flash cookies, 214, 217

flash drives, 106

flash memory cards
 exFAT, 464
 FAT, 464
 reading, 111–112
 UltraBlock Forensic Card Reader and Writer, 111–112

flasher boxes, 409, 418

flashlights, 141

FLETC (Federal Law Enforcement Training Centers), 21, 29

Flickr, 466

floppy disks, 116–118, 121

Foller.me, Twitter analytics, 205

forensically sound, defined, 2

forensics. See also cellphone forensics; digital forensics; iPhone forensics; Mac forensics; network forensics; photo forensics; vehicle forensics

accountants, 29
 Android OS, 398
 anti-forensics, 365
 COFEE, 72
 defined, 2
 going wrong, admissibility of evidence, 296
 imaging software, 36, 143, 144
 AXIOM, 145
 BlackLight, 150
 differences between tools, 143–144
 DriveSpy, 144
 E01 file format, 150, 171
 EnCase, 150
 EnScript, 150, 171
 F-Response, 145
 FTK, 7, 145, 149–150
 FTK Imager, 145, 146–149
 Guidance Software (opentext), 150
 ILook, 144
 Mac Marshal, 150
 Mobilyze, 145
 PALADIN, 145
 TSK, 144
 WinHex, 144
 X-Ways Forensics software, 144

routers, 207–208, 328, 366
 SIM cards, 385–388
 tablets, 413
 tools, documenting use of, 236

forensics laboratories (computers), 126, 170
 accessing, 155
 auditing access, 156
 data access, 155–156
 determining laboratory location, 157

- physical security, 156
- sign-in sheets, 156
- antivirus software, 151
- ASCLD/LAB, 127–129, 171
- budgets, 154
- cabinets, 137
- cloning devices, 137
- digital cameras, 141–142
- email preparation laboratories, 131
- energy requirements, 153
- ergonomics, 154
- evidence
 - evidence acquisition laboratories, 131
 - evidence bags, 142
 - evidence labels, 143
 - evidence lockers, 136, 171
- extracting evidence from devices, 157
 - ATM skimmers, 166–167, 171
 - dd command, 157–158
 - EGREP, 160–161, 171
 - FGREP, 161–162, 171
 - GREP, 158–160, 172
 - GREP, check fraud searches, 165–166
 - GREP, expressions, 162–163
 - GREP, financial fraud searches, 163–165
 - magstripe readers, 166–167, 172
 - parasites, 166, 172
 - skimmers, 166–168
 - steganalysis, 168, 172
 - steganography, 168–169, 172
- Faraday rooms, 135
- field kit storage units, 134–135
- flashlights, 141
- guidelines/standards, 127–130
- harvest drives, 140
- imaging software, 143, 144
 - AXIOM, 145
 - BlackLight, 150
 - differences between tools, 143–144
 - DriveSpy, 144
 - E01 file format, 150, 171
 - EnCase, 150
 - EnScript, 150, 171
 - F-Response, 145
 - FTK, 7, 145, 149–150
 - FTK Imager, 145, 146–149
 - Guidance Software (opentext), 150
 - ILook, 144
 - Mac Marshal, 150
 - Mobilyze, 145
 - PALADIN, 145
 - TSK, 144
 - WinHex, 144
 - X-Ways Forensics software, 144
- inventory control, 131
- ISO/IEC 17025.2017, 129
- laboratory information management systems, 131–132
- layout of, 132–133
- managing, 154–155
- password-cracking software, 151
- photo forensics, 152
 - Adroit forensics, 153
 - evidence, 152–153
 - EXIF data, 152
 - file formats, 152
 - metadata, 152
- private-sector computer forensics laboratories, 130
- safety, 153–154
- security, physical security, 156
- SIM card readers, 139–140
- SWDGE, 129–130, 172
- toolkits, 141
- VMware, 151

web hosting, 132
 workbenches, 134, 172
 workstations, 133
 write-blockers, 137–139

foreperson (juries), 260, 307

Fourth Amendment (U.S. Constitution), 265–266

certiorari, 266, 306
 exclusionary rule, 266, 307
 fruit of the poisonous tree, 266, 278, 308
Katz v. United States, 389 U.S. 347 (1967), 266
O'Connor v. Ortega, 480 U.S. 709 (1987), 266
Olmstead v. United States, 277 U.S. 438 (1928), 266
 search warrants, 309
 court orders, 272, 307
 digital surveillance, 272–273
 email, 267
 GPS tracking, 273–276
 MLB and BALCO, 268
 pen registers, 272–273, 308
 probable cause, 267, 309
 Smith v. Maryland, 442 U.S. 735 (1979), 272–273
 traffic stops, 277–279
 United States v. Daniel David Rigmaiden, 844 F.Supp.2d 982 (2012), 272–273
 United States v. Leon, 468 U.S. 897 (1984), 267
 United States v. Warshak, 562 F. Supp. 2d 986 (S.D. Ohio 2008), 267
 United States v. Ziegler, 267
 warrantless searches, 269
 Arizona v. Gant, 2009, 271, 278
 case studies, 271
 DOJ, 268

exigent circumstances, 268, 307
Horton v. California, 269
 "knock and talk" 269, 308
People v. Diaz, 271
 plain error, 270, 308
 plain view doctrine, 269, 308
Riley v. California, 271
 Rules of Criminal Procedure, 270, 309
 search incident to a lawful arrest, 271
 standing warrants, 271
United States of America, Plaintiff-Appellee, v. Russell Lane WALSER, Defendant-Appellant. No. 01–8019, 269–270
United States v. Carey, No. 14–50222 (9th Cir. 2016), 269, 270
United States v. Mann (No. 08–3041), 270–271
United States v. McConney, 728 F.2d 1195, 1199 (9th Cir.), 268
Weeks v. United States, 232 U.S. 383 (1914), 266

FPLMN (Forbidden Public Land Mobile Networks), 386–387, 418

FragView, 234

frames, 114, 121

Franklin, Benjamin, 253

fraud

check fraud
 Federal Reserve Bank reference list, 165
 GREP searches, 165–166
 financial fraud
 GREP searches, 163–165
 IIN matrix, 163
 MII charts, 163
 OLAF, 303
 PBX, 347–348

FRCP (Federal Rules of Civil Procedure), 236, 290, 307

FRE (Federal Rules of Evidence), 289–290, 307

- best evidence rule, 292–293, 306
- depositions, 290, 307
- expert witnesses, 290–291
- FRCP, 290
- hearsay, 290, 291–292, 308
- photo forensics, 470

FRED workstations, 153**Freenet, Dark Web investigations, 186****F-Response, 145****fruit of the poisonous tree, 266, 278, 308*****Frye v. United States*, 288–289****FTK (Forensic Toolkit), 7, 145****FTK Imager, 53–56, 145****FTK Registry Viewer, 62****FTL (File Translation Layer), 103, 121****fusion centers**

- history of digital forensics, 18–19
- HSIN-SLIC, 208, 217

Fusion Drives (Apple), 491, 494, 533

G

Galaxy (Samsung), 393**garbage collection, 102, 103, 121****Gargol, Brittney, 463****Gatekeeper (macOS), 502–503, 533****gateways (default), 321, 365****gathering evidence, Windows 8.1, 81–82****GDPR (General Data Protection Regulation), 130, 298–301*****General Framework for Secured IoT Systems (NISC)*, 573****Genesis Blocks, 189, 217****geodata, social networking websites, 202–203****Geotab GO, 585****geotags, 203, 217****GET method, 437, 457****GIF files, 469, 475****global satellite service providers, 410****Globestar, 410****glossaries (reports), 241–242****GMDSS (Global Maritime Distress & Safety Services), 410****GMT (Greenwich Mean Time), 237–238, 246****Goldstein, Emmanuel, 15****Google Alerts, searching for stolen property, 197****Google Groups, 201****Google Hangouts, 200****GoPro, 583****Gorshkov, Vasily, 210, 271****GPRS (General Packet Radio Service), 384–385, 418****GPS (Global Positioning Systems), 29****in images, 7****tracking****Assisted GPS, 414, 417****case studies, 414****Enhanced 911, 414, 417****mobile forensics, 413–414****PSAP, 414, 419****search warrants, 273–276****track logs, 414, 420****trackpoints, 414, 420****waypoints, 414, 420****grand juries, 308****graphics****BMP files, 469, 474****comprehensive reports, including in, 238****DNG, 469, 474****file types, overview of, 467–468****GIF files, 469, 475****JPEG files, 468, 475****lossless compression, 152, 172**

- lossy compression, 152, 172, 475
- megapixels, 467–468, 475
- pixels, 467–468, 475
- PNG files, 469, 475
- raster-based graphics, 152, 172, 467–468, 475
- RAW files, 468–469, 475
- TIFF files, 469, 475
- tumbcache.db, 469
- vector graphics, 468, 475

GrayKey, 406**Greig, Catherine, 204****GREP (Global Regular Expressions Print), 158–160, 172**

- check fraud searches, 165–166
- EGREP, 160–161, 171
- expressions, 162–163
- FGREP, 161–162, 171
- financial fraud searches, 163–165

Grindr application (app), 445–450**grouping files, Windows 7, 78****GSM (Global System for Mobile Communications), 384, 418****GuerillaMail, 179–180****Guidance Software (opentext), 150****H**

hacktivists, 529**Halligan, Jim, 198****Halligan, Ryan, 559****Hamilton, Alexander, 253****Hammond, Richard, 583****handsets**

- cellphone forensics, 406
- cellphones, 389

Hansa, Dark Web investigations, 188**happy slapping, 558, 564****hard disk drives. See HDD****hard disks**

- actuator arms, 37–38
- capacity, determining, 38
- cylinders, 38
- disk geometry, 38
- layout of, 37–38
- page files, 39
- Pagefile.sys, 39
- physical layout of, 36–37
- platters, 37–38
- spindles, 37–38

hard/soft handoffs, 377, 418, 420**harvest drives, 140****HCR (HKEY_CURRENT_USER), 363****HCU (HKEY_CURRENT_CONFIG), 363****HDD (Hard Disk Drives), 93**

- allocation blocks, 489–490, 531
- cloning devices
 - Disk Jockey PRO Forensic Edition, 98–101
 - ImageMASter Solo IV Forensic, 101
- external hard drives, 107–108
- HPA, 99, 100, 121
- IDE, 93, 121
- PATA
 - cloning disks, 97
 - disk images, 97
- SATA, 121
 - cabling, 93, 97
 - cloning disks, 97
 - disk images, 97
 - drives, sizes of, 96–97
 - eSATA connectors, 96, 121
- SCSI, 93–94, 122
- worksheets, documenting investigations, 232
- write-blockers, 101, 107–108, 109, 112, 114, 122

headers

- alternative volume headers, 489–490, 532
- IPv4 headers, 330–331
- TCP/IP headers, 344
- volume headers, 489–490, 534

Health application (app), Apple, 486–487, 530**hearsay, 290, 291–292, 308****HEIF (High Efficiency Image Format), 523, 533****hexadecimal numbers**

- conversion table, 42–43
- Data Link Escape, 45
- hex converters, 45
- hex editors, 45–46
- hexadecimal to ASCII conversion, 44–45
- hexadecimal to decimal file conversion, 43
- hexadecimal to file type conversion, 47

HFS (Hierarchical File Systems), 489, 533**HFS+489–490, 533****hibernation files (macOS), 501****HIDS (Host-based Intrusion Detection Systems), network forensics, 338****high schools, digital forensic training, 22****history of digital forensics, 14–15, 27–28**

- 1980s, 15
- 1990s, 15–19
- 2000s, 20
- Amber Alert Bill, 16–17
- DHS, 16–17
- DoD, 16
- ECTF, 16–17
- encryption, 20
- FARC, 16
- FBI, 15
- fusion centers, 18–19
- INTERPOL, 17–18
- IoT, 20
- IRS, 16
- NCMEC, 15

PC, 15

PROTECT Act, 16–17

RCFL, 18–19

Snowden, Edward, 20

USSS, 16–17

virtual currencies, 20

History.plist, 504–505**HITECH Act, 210–211****HKCC (HKEY_CURRENT_CONFIG), 61****HKCR (HKEY_CLASSES_ROOT), 60, 363****HKCU (HKEY_CURRENT_USER), 60–61****HKLM (HKEY_LOCAL_MACHINE), 61, 363****HKU (HKEY_USERS), 61, 363****HLR (Home Location Register), 382, 418****Hochron, Det. Brett, 586–587****Holden, Thomas Jane, 460–461****HootSuite, 196*****Horton v. California*, 269****hosts files, 327–328, 365****HPA (Host-Protected Areas), 99, 100, 121****HSDN (Homeland Security Data Network), 208, 217****HSIN-SLIC (Homeland Security Interaction-State and Local Fusion Centers), 208, 217****HTTP (Hypertext Transfer Protocol), 365**

GET method, 437, 457

network forensics, 319–320

hubs, 324, 365**hung juries, 261, 308****Huntington Beach Jane Doe, 1968, 460–461****Hyberfil.sys, 68****I****I2P (Invisible Internet Project), Dark Web investigations, 186****IANA (Internet Assigned Numbers Authority), 337, 365**

IP addresses,

iBeacon, 518, 533

iBoot, 513, 533

ICAID (INTERPOL Child Abuse Image Database), 18

ICANN (Internet Corporation for Assigned Names and Numbers), 328

ICCID (Integrated Circuit Card ID), 381–382, 418

iCloud, 517–518, 533

iCloud Keychain, 504, 533

IDE (Integrated Drive Electronics), 94–95, 121

iDEN (Integrated Digital Enhanced Networks), 385, 418

identification

App ID, 428, 457

Apple ID, 510

bundle ID, 428, 457

Catalog ID, 489–490, 532

Face ID, 517, 532

FCC-ID, 380, 404, 418

ICCID, 381–382, 418

Touch ID, 515–516, 534

identities

generating

Bitcoin, 178

email, 178

Fake Name Generator, 179

malware protection, 178

sockpuppets, 178

virtual currencies, 178

masking

Bluffmycall.com,
181–182

online proxies, 183–184

Spy Dialer, 182–183

telephone carriers, 183

wiretaps, 183

theft, 210

IDS (Intrusion Detection Systems), 365

HIDS, 338

IPS, 339

network forensics, 338

NIDS, 338

NNIDS, 338

IIN (Issuer Identification Numbers), 163, 172

ILook, 144

IM (Instant Messaging)

acronyms, 198–199

AIM messages, 200

background searches, 197–200

DeadAim, 198

Discord, 200

evidence, 199–200

Google Hangouts, 200

IRC, 197–198, 217

Mibbit, 197

Skype, 200

XMPP, 199

ImageMASter Solo IV Forensic, 101

images. See also photo forensics

BMP files, 469, 474

brightness, 471, 474

color balance, 471, 474

comprehensive reports, including in, 238

contrast, 471, 474

cropping images, 471, 474

as digital evidence, 7–8

DMG images, 494, 498

DNG, 469, 474

enhanced images, photo forensics, evidence
admissibility, 471

evidence admissibility, 470–473

analog vs digital photography, 470–471

enhanced images, 471

FRE, 470

SWGDE, 470

- fake/altered images, 471
 - file metadata, 7
 - file types, overview of, 467–468
 - FTK application and, 7
 - GIF files, 469, 475
 - GPS data, 7
 - HEIF, 523, 533
 - JPEG files, 468, 475
 - linear filtering, 471, 475
 - lossless compression, 152, 172
 - lossy compression, 152, 172, 475
 - megapixels, 467–468, 475
 - pixels, 467–468, 475
 - PNG files, 469, 475
 - raster-based graphics, 152, 172, 467–468, 475
 - RAW files, 468–469, 475
 - sleepimage files, 501, 534
 - sparse images, 534
 - SWGIT, 471, 475
 - TIFF files, 469, 475
 - tumbcache.db, 469
 - vector graphics, 468, 475
 - X-Ways Forensics software and, 7–8
- imaging disks, 97, 121**
- imaging software (forensic), 36, 143, 144**
- AXIOM, 145
 - BlackLight, 150
 - differences between tools, 143–144
 - DriveSpy, 144
 - E01 file format, 150, 171
 - EnCase, 150
 - EnScript, 150, 171
 - F-Response, 145
 - FTK, 7, 145, 149–150
 - FTK Imager, 145, 146–149
 - Guidance Software (opentext), 150
 - ILook, 144
 - iPhone, 512
 - Mac Marshal, 150
 - Mobilyze, 145
 - PALADIN, 145
 - TSK, 144
 - WinHex, 144
 - X-Ways Forensics software, 144
- IMEI (International Mobile Equipment Identities), 378–379, 381–382, 418**
- impersonation, 558, 564**
- improper/proper statements (reports), 241**
- IMSI (International Mobile Subscriber Identities), 381, 418**
- inculpatory evidence, 2, 29**
- Index.dat, 215, 217**
- indexing (Windows search engine), Vista, 66**
- Indian legal system, 304**
- indictments, 308**
- InfraGard, 21–22, 29**
- initialization (macOS), 495, 533**
- Inmarsat PLC, 410**
- InPrivate Browsing, Internet Explorer, 76–77**
- Instagram, 466**
- intellectual property, E.U. legal system, 302**
- intent, email, 5–6**
- intermediate appellate courts, 257**
- international databases, law enforcement access, 209**
- international numbering plans, 382–383**
- Internet Explorer, InPrivate Browsing, 76–77**
- Internet searches/websites visited, 9**
- INTERPOL, 29**
- history of digital forensics, 17–18
 - MIND/FIND, 209, 217
 - photo forensics, 471–473
- Intrusion Kill Chains, 350**
- C2, 352
 - delivery, 352

- DLL side-loading, 353
 - exfiltration, 352
 - exploitation, 352
 - job postings, 351
 - persistence, 353
 - press releases, 351
 - reconnaissance, 350–352
 - remediation, 354
 - tech forums, 351
 - TTP, 352–353
 - weaponization, 352
 - YARA, 353
- inventory control, 131**
- investigating**
- applications (apps), 457
 - communication applications, 453–456
 - dating applications, 441–450
 - Debookee, 433–441
 - dynamic analysis, 431–433
 - JSLint, 430–431
 - pcap files, 431–432, 457
 - rideshare applications, 450–453
 - SQLite database, 427–431
 - static analysis, 427–431
 - wireless monitoring, 431–433
 - background searches, 191–192
 - blogs, 202
 - dynamic IP addresses, 207
 - Google Groups, 201
 - IM, 197–200
 - IPv4 addresses, 206–207
 - law enforcement access, 208–209
 - locating suspects, 207
 - metadata, 207
 - personal information, 192–195
 - personal interests, 195–196
 - professional networks, 205–206
 - public records, 206
 - router forensics, 207–208
 - social media, 195–196
 - social networking websites, 202–205
 - stolen property, 196–197
 - usenet groups, 200–201
 - user groups, 196
 - Dark Web investigations
 - AlphaBay, 187–188
 - Freenet, 186
 - Hansa, 188
 - I2P, 186
 - marketplaces, 186–188
 - Operation Bayonet, 187–188
 - OSINT Framework, 184
 - PlayPen, 187
 - Silk Road, The, 187
 - Tails, 185, 218
 - Tor, 184–185, 218
 - documenting investigations, 224, 245
 - Chain of Custody forms, 229–230
 - Cop App application (app), 235
 - crime scenes, 226–234
 - CSI equipment, 228–229
 - Digital Forensics Reference application (app), 235
 - evidence, obtaining from ISP, 224–225
 - evidence lists, 226–227
 - expert witnesses, 242–244, 246
 - Federal Rules of Evidence application (app), 236
 - FragView, 234
 - FRCP application (app), 236
 - hard disk drive worksheets, 232
 - lay witnesses, 243, 246
 - Lock and Code application (app), 235
 - Network Analyzer, 235
 - photos, 231

- preservation orders, 225, 246
- reports, 236–242
- on-scene examinations, 227–228
- seizing evidence, 227
- server worksheets, 233–234
- System Status application (app), 235
- tagged evidence, 229
- tools/applications, 234–236
- network attacks, 357
 - AmCache, 357–358
 - EDR, 359
 - Kibana, 359
 - Log2Timeline, 359
 - RAM, 357
 - SANS SIFT workstation, 360–361
 - ShellBags, 358
 - ShimCache, 358
 - VSC, 358
 - Windows Registry, 361–363
- online communications
 - AXIOM, 212
 - cookies, 214
 - screen captures, 212–213
 - video, 213–214
 - websites visited, 215
- online crime, 209
 - CPI, 211
 - credit cards for sale, 210
 - cyberbullying, 211
 - electronic medical records, 210–211
 - identity theft, 210
 - social networking, 211–212
- online investigations, 176–177, 216
- purpose of investigation (reports), 240
- undercover investigations, 177–184, 218
 - anonymity, 181–184
 - background searches, 177

- generating email accounts, 179–181
- generating identities, 178–179
- sting operations, 178
- surveillance, 177–178
- warrants, 178
- wiretaps, 178, 183
- virtual currencies, 188–189
- website evidence, 189
 - website archives, 189–190
 - website statistics, 190–191

investigative details connected to the case (reports), 241

Investigative Powers Act of 2016, 302

investigator skills

- communication skills, 11
- computer science knowledge, 10–11
- confidentiality, 12
- continuous learning, 12
- legal expertise, 11
- linguistic abilities, 12
- programming, 12

IOC (Indicators of Compromise), 354, 357

- \$USN_Journal, 355
- DLL files, 354
- email, 354
- event logs, 355–357
- MFT, 355
- MRU lists, 356
- ports, 355
- Prefetch files, 355
- PSExec, 356
- RAM, 357
- Registry keys, 354
- ServiceDLL, 354
- svc.host.eve, 354
- System32, 355
- UserAssist, 357

IOReg Info (Blackbag Technologies), 495–496

iOS

- Apple ID, 510
- Data Protection, 509, 532
- encryption, 509–510
- iOS 13, 508–509
- media partitions, 508, 533
- root partitions, 508, 534
- security, 509–510
- System Software Personalization, 508, 534
- Tinder SQLite database, 427–429
- UDID, 534
- USB Restricted Mode, 510, 534

IoT (Internet of Things), 10, 572–573, 588, 589

- 5G, 573–575
- action cameras, 583
- Alexa virtual assistant, 578–579
- Apple Watch, 581–583
- botnets, 577
- cryptojacking, 577–578, 588
- CUPS, 574, 588
- D2D, 574, 589
- fitness trackers, 579–580
- General Framework for Secured IoT Systems*, 573
- history of digital forensics, 20
- law enforcement
 - ANPR, 585, 588
 - BWC, 584, 588
 - C-V2X, 585, 588
 - drones, 584
 - facial recognition, 584
 - police safety, 583–585
 - police vehicles, 585
 - telematics, 585, 589
- MEC, 574, 589
- micro-chipping, 579
- requirements, 573
- Ring doorbell, 585

- Shodan, 576–577
- smart holster sensors, 584, 589
- U.K. Code of Practice for Consumer Internet of Things Security*, 573
- Vo5G, 575, 589
- Wi-Fi mesh networks, 576, 589

IP addresses

- dynamic IP addresses, 207, 217
- IANA and, 337
- IP Address expressions (GREP), 162–163
- IPv4, 217
 - background searches, 206–207
 - headers, 330–331, 365
 - network forensics, 330–331
- IPv6, network forensics, 337
- reserved IP addresses, 334
- TCP/IP headers, 344
- VoIP
 - network forensics, 346, 367
 - STUN, 348

IP subnet masks, calculating, 334–335**iPad, 485, 487, 511, 530****iPhone, 483–484, 511**

- APOLLO tool, 525–526
- Apple Configurator, 526–527, 532
- backups, 517, 522–523
- batteries, 527
- checkm8, 522
- checkra1n, 522
- DFU Mode, 512–513
- enterprise deployments, 526–527
- Face ID, 517, 532
- Find My iPhone feature, 529
- iBeacon, 518, 533
- iBoot, 513, 533
- iCloud, 517–518, 533
- imaging software, 512
- iPhone 3G, 513

- iPhone 3GS, 514
 - iPhone 4, 514
 - iPhone 5, 514
 - iPhone 5C, 514–515
 - iPhone 5S, 514
 - iPhone 6, 514–515
 - iPhone 6 Plus, 514–515
 - iPhone 11, 516
 - iPhone 11 Pro, 516
 - iPhone 11 Pro Max, 516
 - KTX Snapshots, 523–524
 - Location Services, 518–522, 533
 - MAC addresses, finding, 337
 - Mail, 518
 - modes of operation, 512–513
 - Notes application (app), 523
 - original iPhone, 513
 - photos, 518, 523–524
 - Recovery Mode, 513, 534
 - Safari web browser, 518
 - Significant Locations, 521
 - SIM cards, 513
 - stolen iPhone case study, 529
 - Touch ID, 515–516, 534
 - user events, 525
 - iPod, 482–483, 510–511**
 - iPod Touch, 482–483**
 - IPS (Intrusion Prevention Systems), network forensics, 339**
 - IPv4 (IP Addressing version 4), 365**
 - IR (Incident Response), 348–349, 364**
 - IRC (Internet Relay Chats), 197–198, 217**
 - Iridium Communications, Inc.410**
 - IRS (Internal Revenue Service)**
 - history of digital forensics, 16
 - virtual currencies, 188
 - IsAnybodyDown website, photo forensics, 464**
 - ISO/IEC 17025.2017, 129**
 - ISP (In-System Programming), Android OS, 396, 418**
 - ISP (Internet Service Providers), evidence, obtaining, 224–225**
 - ISPC (International Signal Point Codes), 382, 418**
 - ITU (International Telecommunication Union), 384, 418**
 - Ivanov, Alexey, 210, 271**
- ## J
-
- Jabbr. See XMPP**
 - Jablin, Fred, 414**
 - Jackson, Michael, 529**
 - job opportunities/postings**
 - digital forensics, 13–14
 - Intrusion Kill Chains, 351
 - Jones, Antoine, 274–276**
 - journaling**
 - defined, 51
 - macOS, 498
 - JPEG files, 468, 475**
 - JSLint, 430–431**
 - JTAG (Joint Test Action Group), 394–395, 418**
 - Judex, 297, 308**
 - judges, 255, 308**
 - JumpLists, 69**
 - jurisdiction, 256, 308**
 - trial courts of general jurisdiction, 258–259
 - trial courts of limited jurisdiction, 258
 - juries, 253, 260, 308**
 - contempt of court, 260
 - foreperson, 260, 307
 - grand juries, 308
 - hung juries, 261, 308
 - indictments, 308

sequestration, 260, 308

voir dire, 260, 309

juvenile courts, 258, 308

K

Kagan, Justice Elena, 275

Kali Linux, 315

Kaminski, John, 115

***Katz v. United States*, 389 U.S. 347 (1967), 266**

Keating, Stephen, 463–464

Kee, Eric, 471

KEK (Key Encryption Keys), 491, 533

Kelley, Det. Coby, 414

Kernel, David, 183

kernels, 48

keybags, 491–492, 533

Keychain (macOS), 503

Khan, Samir, 202

Khavari, Hussein, 530

Kibana, 359

"knock and talk"269, 308

Krieger, Mike, 466

KTX Snapshots, 523–524

***Kumho Tire Co. v. Carmichael*, 289**

L

laboratories (computer forensics), 126, 170

accessing, 155

auditing access, 156

data access, 155–156

determining laboratory location, 157

physical security, 156

sign-in sheets, 156

antivirus software, 151

ASCLD/LAB, 127–129, 171

budgets, 154

cabinets, 137

cloning devices, 137

digital cameras, 141–142

email preparation laboratories, 131

energy requirements, 153

ergonomics, 154

evidence

evidence acquisition laboratories, 131

evidence bags, 142

evidence labels, 143

evidence lockers, 136, 171

extracting evidence from devices, 157

ATM skimmers, 166–167, 171

dd command, 157–158

EGREP, 160–161, 171

FGREP, 161–162, 171

GREP, 158–160, 172

GREP, check fraud searches, 165–166

GREP, expressions, 162–163

GREP, financial fraud searches, 163–165

magstripe readers, 166–167, 172

parasites, 166, 172

skimmers, 166–168

steganalysis, 168, 172

steganography, 168–169, 172

Faraday rooms, 135

field kit storage units, 134–135

flashlights, 141

guidelines/standards, 127–130

harvest drives, 140

imaging software, 143, 144

AXIOM, 145

BlackLight, 150

differences between tools, 143–144

DriveSpy, 144

E01 file format, 150, 171

EnCase, 150

- EnScript, 150, 171
- F-Response, 145
- FTK, 7, 145, 149–150
- FTK Imager, 145, 146–149
- Guidance Software (opentext), 150
- ILook, 144
- Mac Marshal, 150
- Mobilyze, 145
- PALADIN, 145
- TSK, 144
- WinHex, 144
- X-Ways Forensics software, 144
- inventory control, 131
- ISO/IEC 17025.2017, 129
- laboratory information management systems, 131–132
- layout of, 132–133
- managing, 154–155
- password-cracking software, 151
- photo forensics, 152
 - Adroit forensics, 153
 - evidence, 152–153
 - EXIF data, 152
 - file formats, 152
 - metadata, 152
- private-sector computer forensics laboratories, 130
- safety, 153–154
- security, physical security, 156
- SIM card readers, 139–140
- SWDGE, 129–130, 172
- toolkits, 141
- VMware, 151
- web hosting, 132
- workbenches, 134, 172
- workstations, 133
- write-blockers, 137–139
- laboratory information management systems, 131–132**
- Ladenburger, Maria, 530**
- lands (CD), 113–114, 121**
- Las Vegas Massacre, 549–550**
- latency, 573, 589**
- law. See also legal systems**
 - Civil law, 254, 306
 - Codified law, 254, 306
 - common law, 254, 306
 - congressional legislation
 - CALEA, 284
 - CLOUD Act, 288
 - Computer Fraud and Abuse Act (18 U.S.C. § 2511), 283
 - Corporate Espionage (18 U.S.C. § 1030(a)(1)), 283–284
 - Digital Millennium Copyright Act (DMCA) (17 U.S.C. § 1201), 286–287
 - Federal Wiretap Act (18 U.S.C. § 2511), 281–282
 - FISA-1978, 282–283
 - PROTECT Act, 286
 - USA PATRIOT Act (H.R. 3162), 14, 16–17, 268, 283, 284–286
 - Constitutional law, 254, 262, 306
 - Louisiana Civil Code Digest of 1808, 254
 - Napoleonic Code, The, 254
 - precedents, 254, 309
 - Regulatory law, 254, 309
 - Roman law, 254
 - Statutory law, 254, 309
 - subpoenas, 309
- law enforcement**
 - ANPR, 585, 588
 - CALEA, 284
 - C-V2X, 585, 588
 - digital forensic training, 21–22

- facial recognition, 584
- Harley the cyber dog, 586–587
- IoT
 - BWC, 584, 588
 - drones, 584
 - police safety, 583–585
 - police vehicles, 585
 - smart holster sensors, 584, 589
- personal information, accessing, 208
 - federal, state, local information exchange, 208–209
 - international databases, 209
 - local law enforcement, 208
 - RTCC, 208
 - telematics, 585, 589
- lay witnesses, 243, 246**
- Layshock et al v. Hermitage School District et al, 264–265***
- LeadsOnline, searching for stolen property, 196**
- LEAP (Local Number Portability Enhanced Analytical Platform), 183**
- Leap Second Bug, 237, 246**
- learning (continuous), digital forensics skills, 12**
- legal expertise (digital forensics skills), 11**
- legal systems, 305–306. See also law**
 - Chinese legal system, 304
 - E.U. legal system, 296–297
 - ACPO, 303
 - child pornography directives, 302–303
 - Court of Justice of the European Union, 297, 307
 - data privacy, 209, 298
 - European Commission, 297
 - European law, origins of, 297–303
 - Europol, 303
 - Facebook, 302
 - GDPR, 298–301
 - intellectual property, 302
 - Investigative Powers Act of 2016, 302
 - Judex, 297, 308
 - legislatures, 297
 - OLAF, 303
 - UK Modern Slavery Act, 301
 - Indian legal system, 304
 - U.S. legal system, 252
 - Articles of the Constitution, 254
 - Bill of Rights, The, 254, 262, 306
 - Civil law, 254, 306
 - Codified law, 254, 306
 - common law, 254, 306
 - Constitutional law, 254, 262, 306
 - criminal defense, 293–295
 - defendants, 253, 307
 - history of, 253–254
 - juries, 253, 308
 - Louisiana Civil Code Digest of 1808, 254
 - motion in limine, 267, 308
 - Napoleonic Code, The, 254
 - Ninth U.S. Circuit Court of Appeal's, 268
 - origins of, 254
- plaintiffs, 130, 172, 253, 309**
 - precedents, 254, 309
 - Regulatory law, 254, 309
 - Roman law, 254
 - Statutory law, 254, 309
 - structure of, 253–254
- subpoenas, 309**
 - U.S. Constitution, 254, 256
 - U.S. court system, overview of, 254–262
- legislatures (E.U.), 297**
- Lewinsky, Monica, 183**
- Linden dollars, 188**
- linear filtering (images), 471, 475**
- linguistic abilities (digital forensics skills), 12**

LinkedIn, background searches, 205
Linux, 315, 317–318
LND (Last Numbers Dialed), 386–387, 418
Locard's Exchange Principle, 4
locating suspects, 207
location of a laboratory, determining, 157
Location Services (iPhone), 518–522, 533
Lock and Code application (app), 235
Log2Timeline, 359
logical file size, defined, 36
logs
 DHCP servers, 322–324
 event logs, IOC, 355–357
 track logs, GPS devices, 414, 420
 trackpoints, GPS devices, 414, 420
lossless compression, 152, 172
lossy compression, 152, 172, 475
Louisiana Civil Code Digest of 1808, 254
Lounsbury, Det. Mark, 296

M

Mac (Apple), 481

About This Mac feature, 527
 AFF4, 492, 531
 APFS, 490–491, 532
 AFF4, 492, 531
 APFS Free Queue, 492, 532
 copy-on-write feature, 491, 532
 data cloning, 491, 532
 encryption, 491–492
 keybags, 491–492, 533
 metadata, 491
 snapshots, 493, 534
 space sharing, 492, 534
 T2 security chip, 492
 tmutil snapshot [enter], 493
 App .db files, 456

Apple Configurator, 526–527, 532
 Boot Camp, 92, 120, 489, 532
 Cache.db, 505
 deleted files, 498
 DMG images, 494, 498
 email files, 501
 enterprise deployments, 526–527
 Epoch Converter, 497, 521
 Epoch time, 496–497
 forensics, 480, 494, 527–528, 531
 AFF4, 492, 531
 case studies, 529–530
 deleted files, 498
 DMG images, 494, 498
 email files, 501
 Epoch Converter, 497, 521
 Epoch time, 496–497
 hibernation files, 501
 initialization, 495, 533
 IOReg Info, 495–496
 iPhone, 511–526
 journaling, 498
 PLists, 455, 499–501, 504–506
 PMAP Info, 495–496
 sleepimage files, 501, 534
 Spotlight feature, 494–495, 534
 SQLite database, 501, 505
 Fusion Drives, 491, 494, 533
 HFS, 489, 533
 HFS+489–490
 hibernation files, 501
 initialization, 495, 533
 IOReg Info, 495–496
 journaling, 498
 MAC addresses, finding, 337
 Mac OS Extended. See HFS+
 MFS, 489, 533

- PLists, 455, 499–501
 - Cookies.plist, 505
 - Downloads.plist, 505
 - History.plist, 504–505
 - TopSites.plist, 506
- PMAP Info, 495–496
- Quick Look, 494, 499, 534
- screen captures, 212–213
- sleepimage files, 501, 534
- Spotlight feature, 494–495, 534
- SQLite database, 501
 - Cache.db, 505
- T2 security chip, 492
- Target Disk Mode, 506–507
- Terminal Window, 500
- MAC addresses**
 - finding, 336–337
 - network forensics, 335–337
- Mac Marshal, 150**
- Mac mini, 481–482**
- Mac OS Extended. See HFS+**
- macOS, 502**
 - Cache.db, 505
 - Catalina, 502–503
 - Cocoa, 499, 521, 522, 532
 - Cookies.plist, 505
 - deleted files, 498
 - Disk Utility, 503
 - displays (multiple), support for, 504
 - DMG images, 494, 498
 - Downloads.plist, 505
 - email files, 501
 - Epoch Converter, 497
 - Epoch time, 496–497
 - FileVault, 503, 532
 - Gatekeeper, 502–503, 533
 - hibernation files, 501
 - History.plist, 504–505
 - iCloud Keychain, 504, 533
 - initialization, 495, 533
 - IOReg Info, 495–496
 - journaling, 498
 - Keychain, 503
 - notifications, 504, 533
 - Objective-C, 499, 533
 - PLists, 455, 499–501, 504–506
 - PMAP Info, 495–496
 - Safari web browser, 504
 - Cache.db, 505
 - Cookies.plist, 505
 - Downloads.plist, 505
 - History.plist, 504–505
 - TopSites.plist, 506
 - webpage reviews, 504–505
 - sleepimage files, 501, 534
 - Spotlight feature, 494–495, 534
 - SQLite database, 501
 - tags, 504
 - Target Disk Mode, 506–507
 - TopSites.plist, 506
- Magnet Forensics, 399**
- magnetic tapes, 119, 121**
- magstripe readers, 166–167, 172**
- Mail, iPhone, 518**
- mail expire, 180**
- Mailinator, 181**
- Major League Baseball (MLB), 561–562, 563**
- malware**
 - security, 178
 - VPN, 178
- managing computer forensics laboratories, 154–155**
- Marbury v. Madison, 256, 262**
- marketplaces, Dark Web investigations, 186–188**

- Mason, George, 262**
- Master Boot Code, 49**
- Master Partition Tables, 49**
- Mattel v. MGA Entertainment, Inc.* 6**
- MBR (Master Boot Records), 49**
- MCC (Mobile Country Codes), 381, 418**
- McCaffrey, Kate, 529**
- McIntyre v. Ohio Elections Commission*, 514
U.S. 334, 357 (1995), 287**
- MEC (Multi-access Edge Computing), 574,
589**
- media partitions (iOS), 508, 533**
- medical records (electronic)**
 - HITECH Act, 210–211
 - online crime, 210–211
- megapixels, 467–468, 475**
- Megaproxy, 183**
- MEID (Mobile Equipment Identifiers), 379, 418**
- Meier, Megan, 559**
- Melendez-Diaz v. Massachusetts*, 281**
- memory**
 - CD-ROM, frames, 114, 121
 - cellphones, 389–390
 - flash memory cards
 - exFAT, 464
 - FAT, 464
 - reading, 111–112
 - UltraBlock Forensic Card Reader and
Writer, 111–112
 - Memory Sticks, 110, 121
 - physical memory, Vista, 67
 - RAM, 30, 39, 42, 103–104, 121, 357
 - removable memory, 105
 - ROM, 48
 - virtual memory, 39, 42
 - xD Picture Cards, 111, 122
- Merck, 2017 ransomware attack, 314**
- mesh networks (Wi-Fi), 576, 589**
- metadata**
 - APFS file metadata, 491
 - background searches, 207
 - file metadata, 7, 29
 - photo forensics, 152
 - Vista, 67
- methodologies (reports), 240, 246**
- MFS (Macintosh File Systems), 489, 533**
- MFT (Master File Tables), 52, 355**
- Mibbit, IM background searches, 197**
- micro-chipping, 579**
- Microsoft Edge, 82**
- Microsoft Office, 62–63**
- Microsoft Office 365, 83**
- MiFi (My Wireless Fidelity), 383, 419**
- MII (Major Industry Identifiers), 163, 172**
- Miller v. California*, 413 U.S. 15 (1973), 265**
- MIME (Multipurpose Internet Mail
Extensions), 326, 365**
- MIND/FIND, 209, 217**
- Mirai Botnet, 577**
- misdemeanors, 261, 308**
- Miss Teen USA, photo forensics case
studies, 464**
- MITM (Man-in-the-Middle) attacks, 433, 457**
- MLB (Major League Baseball), 268**
- MMC (MultiMediaCards), 108, 121**
- MMS (Multimedia Messaging Service), 389,
419**
- MNO (Mobile Network Operators), 383, 419**
- mobile applications. See applications**
- Mobile Connect, 575, 589**
- mobile device examination workbenches, 134**
- mobile forensics. See cellphone forensics**
- mobile OS**
 - Android OS, 391, 417
 - ADB, 398, 417
 - Android Auto, 391–392

- applications, 399–400
- Chip-Off, 395–396
- EDL mode, 396–397, 417
- evidence, 394–396
- file systems, 392
- forensics tools, 398
- ISP, 396, 418
- JTAG, 394–395, 418
- partitions, 392–393
- resources, 399
- security, 396
- USB debugging, 398, 420

iOS

- Apple ID, 510
- Data Protection, 509, 532
- encryption, 509–510
- iOS 13, 508–509
- media partitions, 508, 533
- root partitions, 508, 534
- security, 509–510
- System Software Personalization, 508, 534
- Tinder SQLite database, 427–429
- UDID, 534
- USB Restricted Mode, 510, 534

RIM OS, 400, 419

Samsung Galaxy, 393

Symbian OS, 400, 420

Windows 10 Mobile, 400, 420

Mobile Stations, 419

- FCC-ID, 380, 404
- ICCID, 381–382, 418
- IMEI, 378–379, 381–382, 418
- IMSI, 381, 418
- international numbering plans, 382–383
- ISPC, 382, 418
- MCC, 381, 418
- MEID, 379, 418

MSIN, 381, 419

MSISDN, 381, 419

SIM cards, 381–382, 385–388

subsidy locks, 379, 420

TAC, 378, 420

UICC, 379, 420

MOBILedit! Forensic, 407

Mobilyze, 145

monitoring applications (wireless), 431–433

Monster Crawler, searching for stolen property, 197

motion in limine, 267, 308

Moussaoui, Zacharias, 551–555, 563

MRU lists, IOC, 356

MSC (Mobile Switching Centers), 374, 419

MSIN (Mobile Subscriber Identity Numbers), 381, 419

MSISDN (Mobile Subscriber ISDN), 381, 419

MSP (Managed Service Providers), 315, 365

MST (Mountain Standard Time), 237, 246

multiple displays, macOS support, 504

multiplexing, 385, 419

municipal courts, 258, 308

Murray, Dr. Conrad, 529

MVNO (Mobile Virtual Network Operators), 383, 419

MySpace, background searches, 205

N

Nakamoto, Satoshi, 188

Napoleonic Code, The, 254

NAT (Network Address Translation), 333, 348, 366

NCIC (National Crime Information Center), 209, 218, 411–412, 419

NCMEC (National Center for Missing and Exploited Children), 30

history of digital forensics, 15

- photo forensics, 462–463
- URL Initiative, 462–463
- NCTC (National Counterterrorism Center), 208, 217**
- Netcraft, website statistics, 190**
- Network Analyzer, 235**
- network forensics, 314–315, 345–346, 364**
 - APT, 349, 350, 364, 365
 - attacks, investigating, 357
 - AmCache, 357–358
 - EDR, 359
 - Kibana, 359
 - Log2Timeline, 359
 - RAM, 357
 - SANS SIFT workstation, 360–361
 - ShellBags, 358
 - ShimCache, 358
 - VSC, 358
 - Windows Registry, 361–363
 - Cyborg, 349
 - DHCP servers, 321–324, 365
 - DNS protocol, 328
 - DNS servers, 326–327
 - email, 325–326
 - firewalls, 339–340
 - HIDS, 338
 - hosts files, 327–328
 - hubs, 324
 - ICANN, 328
 - IDS, 338
 - Intrusion Kill Chains, 350
 - C2, 352
 - delivery, 352
 - DLL side-loading, 353
 - exfiltration, 352
 - exploitation, 352
 - job postings, 351
 - persistence, 353
 - press releases, 351
 - reconnaissance, 350–352
 - remediation, 354
 - tech forums, 351
 - TTP, 352–353
 - weaponization, 352
 - YARA, 353
 - IOC, 354, 357
 - \$USN_Journal, 355
 - DLL files, 354
 - email, 354
 - event logs, 355–357
 - MFT, 355
 - MRU lists, 356
 - ports, 355
 - Prefetch files, 355
 - PSExec, 356
 - RAM, 357
 - Registry keys, 354
 - ServiceDLL, 354
 - svc.host.eve, 354
 - System32, 355
 - UserAssist, 357
 - IPS, 339
 - IPv4 addresses, 330–331
 - IPv6, network forensics, 337
 - IR, 348–349, 364
 - Kali Linux, 315
 - MAC addresses, 335–337
 - mistakes in, 345
 - networking devices, list of, 316–317
 - NIDS, 338
 - NNIDS, 338
 - OpenPGP, 330
 - OSI model, 341–346
 - packet sniffers, 316, 366
 - PBX, 346–348

- PGP encryption, 329–330
- ports, 340–341
- Promiscuous mode (NIC), 316
- protocol analyzers, 316
- proxy servers, 317
- RAID, 315
- real-time capture/analysis, 315
- retroactive analysis of captured data, 315
- routers, 328
- Secure Data Transmission, 328, 366
- SIP, 348
- SMTP servers, 324–325
- STIX, 349
- STUN, 348
- subnet masks, 332–337
 - calculating, 334–335
 - finding, 335
- TAXII, 349
- tools, 315–316
- Traceroute, 328, 367
- VoIP, 346
- web servers, 317–321
 - HTTP, 319–320
 - scripting languages, 320–321
 - URI, 318
 - web browsers, 318–319
- Network Layer (Layer 3), OSI model, 342, 366**
- networks**
 - attacks, investigating, 357
 - AmCache, 357–358
 - EDR, 359
 - Kibana, 359
 - Log2Timeline, 359
 - RAM, 357
 - SANS SIFT workstation, 360–361
 - ShellBags, 358
 - ShimCache, 358
 - VSC, 358
 - Windows Registry, 361–363
 - backing up to networks, Windows 7, 71–72
 - cellular networks, 417
 - 3GP, 384–385, 416
 - 3GP2, 385, 416
 - 4G, 383
 - 4G LTE Advanced, 383, 416
 - 5G, 384, 573–575, 588
 - ADN, 386–387, 417
 - AuC, 383, 417
 - BSC, 377
 - BTS, 373, 374–377, 417
 - CDMA, 385, 417
 - CDMA2000, 385, 417
 - cell sites, 374, 417
 - EDGE, 384–385, 417
 - EIR, 383, 417
 - FCC-ID, 380, 404
 - FPLMN, 386–387, 418
 - GRPS, 384–385
 - GSM, 384, 418
 - hard/soft handoffs, 377, 418, 420
 - HLR, 382, 418
 - ICCID, 381–382, 418
 - iDEN, 385
 - IMEI, 378–379, 381–382, 418
 - IMSI, 381, 418
 - international numbering plans, 382–383
 - ISPC, 382, 418
 - ITU, 384
 - LND, 386–387, 418
 - locating cell towers/antennas, 375
 - MCC, 381, 418
 - MEID, 379, 418
 - MiFi, 383, 419
 - MMS, 389, 419

- MNO, 383, 419
 - Mobile Stations, 378–383, 419
 - MSC, 374, 419
 - MSIN, 381, 419
 - MSISDN, 381, 419
 - multiplexing, 385, 419
 - MVNO, 383, 419
 - PSTN, 374, 419
 - PUC, 388, 419
 - PUK, 377–378, 388, 419
 - RCS, 389, 419
 - records, 377–378
 - SIM cards, 381–382, 385–388
 - SMS, 388–389, 419
 - subscribers, 377–378, 382–383, 420
 - subsidy locks, 379, 420
 - TAC, 378, 420
 - TDMA, 384, 420
 - TMSI, 382, 386–387, 420
 - UICC, 379, 420
 - UMTS, 385, 420
 - VLR, 382, 420
- W-CDMA, 384, 420**
- Class A networks, subnet masks, 332
 - Class B networks, subnet masks, 332
 - Class C networks, subnet masks, 332
 - DHCP servers, 321–324, 365
 - DNS protocol, 328
 - DNS servers, 326–327
 - firewalls, 365
 - evidence, 340
 - network forensics, 339–340
 - NGFW, 339–340
 - proxy firewalls, 339–340
 - stateful inspection firewalls, 339–340
 - stateless firewalls, 339–340
 - UTM, 339–340
 - FPLMN, 386–387, 418
 - hosts files, 327–328
 - hubs, 324, 365
 - ICANN, 328
 - iDEN, 385, 418
 - IDS, 365
 - HIDS, 338
 - IPS, 339
 - network forensics, 338
 - NIDS, 338
 - NNIDS, 338
 - IPv4
 - address headers, 330–331, 365
 - network forensics, 330–331
 - IPv6, 337
 - MAC addresses, 335–337
 - network masks, 333–334
 - OpenPGP, 330
 - OSI model, 366
 - Application Layer (Layer 7), 345, 365
 - ARP, 342, 365
 - Data Link Layer (Layer 2), 342
 - network forensics, 341–346
 - Network Layer (Layer 3), 342, 366
 - Physical Layer (Layer 1), 341, 366
 - Presentation Layer (Layer 6), 344, 366
 - Session Layer (Layer 5), 344, 366
 - Transport Layer (Layer 4), 343
 - PBX, 366
 - fraud, 347–348
 - network forensics, 346–348
 - PGP encryption, 329–330
 - ports, 340–341, 366
 - proxy servers, 317
 - PSTN, 374, 419
 - reserved IP addresses, subnet masks, 334
 - routers, 328, 366

- routing tables, 342, 366
 - Secure Data Transmission, 328
 - SIP, 348
 - SMTP servers
 - email, 325–326
 - network forensics, 324–326
 - STUN, 348
 - subnet masks, 332, 366
 - calculating, 334–335
 - Class A networks, 332
 - Class B networks, 332
 - Class C networks, 332
 - finding, 335
 - network forensics, 332–337
 - network masks, 333–334
 - reserved IP addresses, 334
 - switches, 324, 367
 - Traceroute, 328, 367
 - VoIP, 346, 367
 - VPN, 178
 - web servers, 317–321
 - Wi-Fi mesh networks, 576, 589
- New York Trial Courts, 258–259**
- New York v. Perez (2011 NY Slip Op 07659)*, 278**
- New York v. Weaver*, 276**
- NewDotNet, 296**
- newsgroups. See usenet groups**
- NGFW (Next Generation Firewalls), 339–340**
- NIC (Network Interface Cards), Promiscuous mode, 316, 366**
- NIDS (Network Intrusion Detection Systems), network forensics, 338**
- NIJ (U.S. Department of Justice)**
- cellphone forensics, 402–403
 - crime scenes, documenting, 226–227
- Ninth U.S. Circuit Court of Appeal's**
- MLB and BALCO, 268
 - United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir.), 268
- NISC, General Framework for Secured IoT Systems, 573**
- NIST (National Institute of Standards and Technology)**
- cellphone forensics, 401–406
 - comprehensive reports, creating, 238
- NLRB (National Labor Relations Board), 176–177**
- NNIDS (Network Node Intrusion Detection Systems), network forensics, 338**
- Notes application (app), iPhone, 523**
- notifications**
- macOS, 504, 533
 - Windows 10, 82
- NotPetya ransomware, 314**
- NTFS (New Technology File System), 51–52**
- defined, 50
 - FTK Imager, 53–56
 - MFT, 52
 - system files, 53
- numbering plans (international), 382–383**
- numbers**
- binary numbers, binary to decimal file conversion, 42
 - decimal numbers
 - binary to decimal file conversion, 42
 - hexadecimal to decimal file conversion, 43
 - hexadecimal numbers
 - conversion table, 42–43
 - Data Link Escape, 45
 - hex converters, 45
 - hex editors, 45–46
 - hexadecimal to ASCII conversion, 44–45

hexadecimal to decimal file conversion, 43

hexadecimal to file type conversion, 47

NW3C (National White Collar Crime Center), 21, 30

NYPD (New York Police Department), Facial Recognition Unit, 473

NYS DFS Rule 23 NYCRR 500, criminal defense, 294–295

O

Objective-C, 499, 533

O'Brien, James, 471

Ochoa III, Higinio O.529

O'Connor v. Ortega, 480 U.S. 709 (1987), 266

OFDMA (Orthogonal Frequency-Division Multiple Access), 575, 589

Office (Microsoft), Microsoft Office, 62–63

Office 365, 83

Ohio v. Johnson, 276

OLAF (European Anti-fraud Office), 303

Olmstead v. United States, 277 U.S. 438 (1928), 266

online communications, capturing

AXIOM, 212

cookies, 214

screen captures, 212–213

video, 213–214

websites visited, 215

online investigations, 176–177, 216

background searches, 191–192

blogs, 202

dynamic IP addresses, 207

Google Groups, 201

IM, 197–200

IPv4 addresses, 206–207

law enforcement access, 208–209

locating suspects, 207

metadata, 207

personal information, 192–195

personal interests, 195–196

professional networks, 205–206

public records, 206

router forensics, 207–208

social media, 195–196

social networking websites, 202–205

stolen property, 196–197

usenet groups, 200–201

user groups, 196

capturing communications

AXIOM, 212

cookies, 214

screen captures, 212–213

video, 213–214

websites visited, 215

Dark Web investigations

AlphaBay, 187–188

Freenet, 186

Hansa, 188

I2P, 186

marketplaces, 186–188

Operation Bayonet, 187–188

OSINT Framework, 184

PlayPen, 187

Silk Road, The, 187

Tails, 185, 218

Tor, 184–185, 218

online crime, 209

CPI, 211

credit cards for sale, 210

cyberbullying, 211

electronic medical records, 210–211

identity theft, 210

social networking, 211–212

undercover investigations

anonymity, 181–184

- background searches, 177
- generating email accounts, 179–181
- generating identities, 178–179
- sting operations, 178
- surveillance, 177–178
- warrants, 178
- wiretaps, 178, 183
- virtual currencies, 188–189
- website evidence, 189
 - website archives, 189–190
 - website statistics, 190–191
- online polls, 558, 564**
- online proxies, 183–184, 218**
- on-scene examinations, documenting crime scenes, 227–228**
- opening statements, 260–261**
- OpenPGP, 330**
- opentext (Guidance Software), 150**
- Operation Bayonet, Dark Web investigations, 187–188**
- Oregon v. Meredith*, 276**
- OS (Operating Systems)**
 - Android OS, 200, 216, 391, 417
 - ADB, 398, 417
 - Android Auto, 391–392
 - Android manifest files, 429–430, 457
 - applications, 399–400
 - Brightest Flashlight, 430
 - Chip-Off, 395–396
 - EDL mode, 396–397, 417
 - emulators, 431, 457
 - evidence, 394–396
 - file systems, 392
 - forensics tools, 398
 - ISP, 396, 418
 - JTAG, 394–395, 418
 - partitions, 392–393
 - resources, 399
 - security, 396
 - USB debugging, 398, 420
 - BIOS
 - defined, 48
 - viewing, 48–49
 - boot process, 48–49
 - bootstrapping, 48
 - defined, 47
 - Disk Signatures, 49
 - End of Sector Markers, 49
 - iOS
 - Apple ID, 510
 - Data Protection, 509, 532
 - encryption, 509–510
 - iOS 13, 508–509
 - media partitions, 508, 533
 - root partitions, 508, 534
 - security, 509–510
 - System Software Personalization, 508, 534
 - Tinder SQLite database, 427–429
 - UDID, 509, 534
 - USB Restricted Mode, 510, 534
 - kernels, 48
 - macOS, 502
 - Cache.db, 505
 - Catalina, 502–503
 - Cookies.plist, 505
 - deleted files, 498
 - Disk Utility, 503
 - displays (multiple), 504
 - DMG images, 494, 498
 - Downloads.plist, 505
 - email files, 501
 - Epoch Converter, 497, 521
 - Epoch time, 496–497
 - FileVault, 503, 532
 - Gatekeeper, 502–503, 533

- hibernation files, 501
- History.plist, 504–505
- iCloud Keychain, 504, 533
- initialization, 495, 533
- IOReg Info, 495–496
- journaling, 498
- Keychain, 503
- notifications, 504, 533
- PList files, 499–501, 504–506
- PMAP Info, 495–496
- Safari web browser, 504–506
- Spotlight feature, 494–495, 534
- SQLite database, 501, 505
- tags, 504, 534
- Target Disk Mode, 506–507
- TopSites.plist, 506
- Mac OS Extended. *See* HFS+
- Master Boot Code, 49
- Master Partition Tables, 49
- MBR, 49
- RIM OS, 400, 419
- ROM, 48
- Samsung Galaxy, 393
- Symbian OS, 400, 420
- UEFI, 48
- Unicode, 47
- Windows 10 Mobile, 400, 420
- Windows OS
 - Microsoft Office, 62–63
 - Safari web browser, 506
 - subnet masks, finding, 335
 - tumbcache.db, 469
 - Vista, 63–68

OSI model, 366

- Application Layer (Layer 7), 345, 365
- ARP, 342, 365
- Data Link Layer (Layer 2), 342

- network forensics, 341–346
- Network Layer (Layer 3), 342, 366
- Physical Layer (Layer 1), 341, 366
- Presentation Layer (Layer 6), 344, 366
- Session Layer (Layer 5), 344, 366
- Transport Layer (Layer 4)
 - SYN Flood attacks, 344
 - TCP, 343–344
 - UDP, 343

OSINT Framework, Dark Web investigations, 184

outing, 558, 564

ownership, email, 5–6

P

packet sniffers, 316, 366

packets (data), 366

Paddock, Steven Craig, 549–550

page files, 39

Pagefile.sys, 39

PALADIN, 145

Palin, Sarah, 183, 210

Paraben StrongHold bags, 403

parasites, 166, 172

partitions

- Android OS, 392–393

- defined, 35–36

- iOS

- media partitions, 508, 533

- root partitions, 508, 534

passwords

- password-cracking software, 151

- PRTK, 151

PATA

- cloning disks, 97

- disk images, 97

Paul, Christopher Neil, 471–473

PBX (Private Branch Exchange), 366

- fraud, 347–348
- network forensics, 346–348

PC (Personal Computers)

- history of digital forensics, 15
- MAC addresses, finding, 336

pcap files, 431–432, 434–435, 457**peer-to-peer payment services, 189****PEI (Prince Edward Island), RCMP, 462****pen registers, 272–273, 308*****People v. Diaz*, 271*****People v Spinelli*, 35 NY2d 77, 81, 278****persistence (Intrusion Kill Chains), 353****persistent cookies, 214, 218****personal data, Indian legal system, 304****personal information**

- background searches, 192–195
- credit cards for sale, 210
- identity theft, 210
- law enforcement access, 208–209

personal interests, background searches, 195–196, 197**PGP encryption**

- network forensics, 329–330
- OpenPGP, 330

photo forensics, 152, 460, 464, 474. See also digital cameras; images

- admissibility of evidence, 470
 - analog vs digital photography, 470–471
 - enhanced images, 471
 - SWGDE, 470
- Adroit forensics, 153
- BMP files, 469, 474
- brightness, 471, 474
- budgets, 154
- case studies, 463, 471
 - Abrahams, Jared, 464
 - Antoine, Cheyenne Rose, 463

Britton, Craig, 464

Cole, Special Agent Jim, 463–464

extortion, 464

Gargol, Brittney, 463

INTERPOL, 471–473

IsAnybodyDown website, 464

Keating, Stephen, 463–464

NYPD Facial Recognition Unit, 473

Paul, Christopher Neil, 471–473

Wolf, Miss Teen USA Cassidy, 464

color balance, 471, 474

contrast, 471, 474

cropping images, 471, 474

DCF, 465, 474

DCIM, 465, 474

digital photography apps, 465–466

DNG, 469, 474

documenting investigations, 231

DSCN, 464, 475

evidence, 152–153, 231

- admissibility, 470

- analog vs digital photography, 470–471

- enhanced images, 471

- SWGDE, 470

EXIF, 152, 466–467, 475

EXIFextracter, 467

ExifTool, 467

Facebook, 461–462, 465

fake/altered images, 471

file formats, 152

file systems, 464–465

file types, overview of, 467–468

Flickr, 464

FRE, 470

GIF files, 469, 475

Holden, Thomas Jane, 460–461

Huntington Beach Jane Doe, 1968, 460–461

- Instagram, 466
- iPhone, 518, 523–524
- JPEG files, 468, 475
- linear filtering, 471, 475
- megapixels, 467–468, 475
- metadata, 152
- NCMEC, 462–463
- pixels, 467–468, 475
- PNG files, 469, 475
- Project VIC, 463–464
- raster-based graphics, 467–468
- RAW files, 468–469, 475
- RCMP, 462
- SnapChat, 466
- social networking, 461–462
- SWGIT, 471, 475
- Ten Most Wanted list (FBI), 460
- TIFF files, 469, 475
- tumbcache.db, 469
- vector graphics, 468, 475
- physical file size, 37**
- Physical Layer (Layer 1), OSI model, 341, 366**
- physical memory, Vista, 67**
- physical security, computer forensics laboratories, 156**
- PIPEDA (Personal Information Protection and Electronic Documents Act), 295**
- pipl, finding personal information, 195**
- Pirate Bay, The, 191**
- pits (CD), 113–114, 121**
- pixels, 467–468, 475**
- plain error, 270, 308**
- plain view doctrine, 269, 308**
- plaintiffs, 130, 172, 253, 309**
- Plaso, 359**
- platters, 37–38**
- PlayPen, Dark Web investigations, 187**
- PlayStation (Sony), 2011 breach, 314**
- PLists, 455**
 - Format files, 533
 - macOS, 499–501
 - Cookies.plist, 505
 - Downloads.plist, 505
 - History.plist, 504–505
 - TopSites.plist, 506
- plutil (property list utility), 499, 533**
- PMAP Info (Blackbag Technologies), 495–496**
- PNG files, 469, 475**
- ports, 366**
 - IOC, 355
 - network forensics, 340–341
- power supplies, UPS, 153, 172**
- PPG (Photoplethysmography), 581, 589**
- precedents, 254, 309**
- predictive coding methodology (reports), 240, 246**
- Prefetch files, 57, 355, 366**
- Presentation Layer (Layer 6), OSI model, 344, 366**
- preservation orders, 225, 246**
- press releases, Intrusion Kill Chains, 351**
- prevalence, email, 6**
- Prince, Phoebe, 558–559**
- Prince Edward Island RCMP, 462**
- privacy (data)**
 - E.U. legal system, 209, 298
 - Indian legal system, 304
- private-sector computer forensics laboratories, 130**
- pro se, 552, 564**
- probable cause, 267, 309**
- probate courts, 258, 309**
- professional certifications, digital forensic training, 22–26**

professional networks

- background searches, 205–206

- LinkedIn, 205

programming

- digital forensics skills, 12

- Unicode, 47

Project VIC, 463–464**Project-a-Phone, 408–409****Promiscuous mode (NIC), 316, 366****proof, burden of, 260–261****proper/improper statements (reports), 241****prosecution, expert witnesses, 244****PROTECT Act, 16–17, 286****protocol analyzers, 316, 366****proxies (online), 183–184, 218****proxy firewalls, 339–340****proxy servers, 317, 366****PRTK (Password Recovery Toolkit), 151****PSAP (Public Safety Access Points), 414, 419****PSExec, IOC, 356****PSTN (Public Switched Telephone Networks), 374, 419****public records**

- background searches, 206

- BRB Publications, Inc.206

PUC (Personal Unblocking Codes), 388, 419**PUK (Pin Unblocking Keys), 377–378, 388, 419****purpose of investigation (reports), 240****Q****QAM (Quadrature Amplitude Modulation), 575, 589****Quick Look, 494, 499, 534****R****Rader, Dennis, 117–118, 555–557, 563****RAID (Redundant Array of Independent**

- Disks), 104, 121, 315**

rainbow tables, 131, 172**RAM (Random Access Memory), 30, 39, 42, 103–104, 121, 357****Ramsey boxes, 403****raster-based graphics, 152, 172, 467–468, 475****RAW files, 468–469, 475****RCFL (Regional Computer Forensics Laboratory), 18–19, 21, 30****RCMP (Royal Canadian Mounted Police), 462****RCS (Rich Communications Service), 389, 419****ReadyBoost, 67****Real Player, 214****real-time capture/analysis, network forensics, 315****reconnaissance (Intrusion Kill Chains), 350–352****records of regularly conducted activity, 291****recovered evidence, types of, 5**

- cellphone forensics, 10

- email, 5

- accessibility, 6

- admissibility, 6

- chain of events, 5

- control, 5–6

- intent, 5–6

- ownership, 5–6

- prevalence, 6

- tampering with evidence, 6

- images, 7–8

- IoT forensics, 10

- video

- CCTV, 8–9

- skimmers, 8

- surveillance video, 8

- websites visited/Internet searches, 9

Recovery Mode (iPhone), 513, 534**Registry (Windows), 59–60, 61**

- analysis, Windows 7, 75
 - data types, 61
 - FTK Registry Viewer, 62
 - HCR (HKEY_CURRENT_USER), 363
 - HCU (HKEY_CURRENT_CONFIG), 363
 - HKCC, 61
 - HKCR, 60
 - HKCR (HKEY_CLASSES_ROOT), 363
 - HKCU, 60–61
 - HKLM, 61, 363
 - HKU, 61
 - HKU (HKEY_USERS), 363
 - Index.dat, 215, 217
 - network attacks, investigating, 361–363
 - Registry Editor, 60
 - registry paths and corresponding files, Windows 7, 76
 - websites visited, viewing, 215
 - Registry Editor, 60**
 - flash drives, 106
 - Registry keys, IOC, 354–357**
 - regularly conducted activity, records of, 291**
 - Regulatory law, 254, 309**
 - remediation (Intrusion Kill Chains), 354**
 - removable memory, 105**
 - reports, documenting investigations, 238, 239**
 - biographies, 240
 - cover pages, 239
 - DST, 236–237, 246
 - electronic media analyzed, 240–241
 - executive summaries, 239
 - exhibits/appendices, 241
 - findings of reports, 241
 - forensic tools, 236
 - glossaries, 241–242
 - graphics, 238
 - investigative details connected to the case, 241
 - methodologies, 240, 246
 - proper/improper statements, 241
 - purpose of investigation, 240
 - structure of, 238–242
 - time zones, 236
 - DST, 236, 246
 - GMT, 237–238, 246
 - MST, 237, 246
 - UTC, 237, 246
 - time zones/DST, 236–238
 - reserved IP addresses, 334**
 - resource forks (HFS), 489, 534**
 - resources, Android OS, 399**
 - restores**
 - Backup and Restore Center, 68
 - restoration points, 71
 - System Restore, 71
 - retroactive analysis of captured data, network forensics, 315**
 - rideshare applications (apps), 450**
 - Riley v. California*, 271**
 - RIM OS, 400, 419**
 - Ring doorbell, 585**
 - RMS (Record Management Systems), 208–209, 218**
 - ROM (Read-Only Memory), 48**
 - Roman law, 254**
 - Rombom, et al. v. Weberman et al.*6**
 - root partitions (iOS), 508, 534**
 - Rountree, Piper, 414**
 - router forensics, 207–208, 328, 366**
 - routes (waypoints), GPS devices, 414, 419**
 - routing tables, 342, 366**
 - RTCC (Real Time Crime Center), 208, 218**
 - Rules of Criminal Procedure, 270, 309**
-
- S**
- SABAM, 302**
 - Safari web browser, 504**

- Cache.db, 505
- Cookies.plist, 505
- Downloads.plist, 505
- History.plist, 504–505
- iPhone, 518
- TopSites.plist, 506
- webpage reviews, 504–505
 - for Windows, 506
- safety, computer forensics laboratories, 153–154**
- Samsung Galaxy, 393**
- SANS SIFT workstation, 360–361**
- SATA (Serial ATA), 121**
 - cabling, 95–96, 97, 121
 - cloning disks, 97
 - disk images, 97
 - drives, sizes of, 96–97
 - eSATA connectors, 96, 121
- satellite communication services, cellphone forensics, 410**
- SaveVid.org, 213**
- screen captures, 212–213**
- scripting languages, network forensics, 320–321**
- SCSI (Small Computer System Interfaces), 93–94, 122**
- SD (Secure Digital) cards, 109–110, 112–113, 121**
- search incident to a lawful arrest, 309**
- search warrants, 178, 309. See also warrantless searches**
 - court orders, 272, 307
 - digital surveillance, 272–273
 - email, 267
 - exclusionary rule, 266, 307
 - GPS tracking, 273–276
 - New York v. Weaver*, 276
 - Ohio v. Johnson*, 276
 - Oregon v. Meredith*, 276
 - state law, 276
 - United States v. Jones*, 274–276
 - United States v. Magana*, 512 F.2d 1169, 1171 [9th Cir. 1975], 274
 - United States v. Dunn*, 480 U.S. 294 (1987), 273
 - United States v. Knotts* 460 U.S. 276 (1983), 273–274
 - United States v. McIver*, 274
 - Washington v. Jackson*, 150 Wash.2d 251, 76 P.3d 217 (Wash. 2003), 276
- MLB and BALCO, 268
- pen registers, 272–273, 308
- probable cause, 267, 309
- Smith v. Maryland*, 442 U.S. 735 (1979), 272–273
- traffic stops, 277
 - Arizona v. Gant*, 278
 - California v. Nottoli*, 277–278
 - Carpenter v. United States*, 278–279
 - New York v. Perez* (2011 NY Slip Op 07659), 278
 - People v. Spinelli*, 35 NY2d 77, 81, 278
 - South Dakota v. Opperman* (1976) 428 U.S. 364 [96 S.Ct. 3092], 277
 - United States v. Daniel David Rigmaiden*, 844 F.Supp.2d 982 (2012), 272–273
 - United States v. Leon*, 468 U.S. 897 (1984), 267
 - United States v. Warshak*, 562 F. Supp. 2d 986 (S.D. Ohio 2008), 267
 - United States v. Ziegler*, 267
- Searchbug, finding personal information, 193**
- searching**
 - background searches, 177, 191–192
 - blogs, 202
 - dynamic IP addresses, 207
 - Google Groups, 201
 - IM, 197–200

- IPv4 addresses, 206–207
- law enforcement access, 208–209
- locating suspects, 207
- metadata, 207
- personal information, 192–195
- personal interests, 195–196
- professional networks, 205–206
- public records, 206
- router forensics, 207–208
- social media, 195–196
- social networking websites, 202–205
- stolen property, 196–197
- usenet groups, 200–201
- user groups, 196
- GREP searches
 - check fraud, 165–166
 - financial fraud, 163–165
- stolen property, 196–197
- Windows Federated Search, 79
- Windows search engine (indexing), Vista, 66
- SEC (Securities and Exchange Commission), 10-day notices, 130**
- sectors, 36**
- Secure Data Transmission, 328, 366**
- security**
 - AES, 67
 - Android OS, 396
 - computer security, 29
 - encryption
 - AES, 67
 - APFS, 491–492
 - FileVault (macOS), 503, 532
 - firewalls, 365
 - evidence, 340
 - network forensics, 339–340
 - NGFW, 339–340
 - proxy firewalls, 339–340
 - stateful inspection firewalls, 339–340
 - stateless firewalls, 339–340
 - UTM, 339–340
 - Indian legal system, 304
 - iOS, 509–510
 - macOS, Gatekeeper, 502–503, 533
 - malware, 178
 - password-cracking software, 151
 - physical security, computer forensics laboratories, 156
 - PRTK, 151
 - steganalysis, 168, 172
 - steganography, 168–169, 172
 - T2 security chip (Apple), 492
 - Windows 8.1, 82
- seizing evidence, 227**
- selling credit cards, 210**
- sequestration of juries, 260, 308**
- servers**
 - DHCP servers, 365
 - ARP requests, 321–322
 - default gateways, 321
 - Event Viewer, 322
 - logs, 322–324
 - network forensics, 321–324
 - subnet masks, 321
 - viewing service activity, 322
 - DNS servers, network forensics, 326–327
 - proxy servers, 317, 366
 - SMTP servers, 366
 - email, 325–326
 - network forensics, 324–326
 - web servers, 9, 30, 367
 - HTTP, 319–320
 - network forensics, 317–321
 - scripting languages, 320–321
 - URI, 318
 - web browsers, 318–319, 367
 - worksheets, documenting investigations, 233–234

- service providers (ISP), obtaining evidence, 224–225**
- ServiceDLL, IOC, 354**
- session cookies, 214, 218**
- Session Layer (Layer 5), OSI model, 344, 366**
- sessions (CD), 114**
- sexting, 558, 564**
- ShellBags, 58, 358**
- ShimCache, 58–59, 358**
- Shodan, 576–577**
- signal jammers, 155–156, 171**
- Significant Locations (iPhone), 521**
- sign-in sheets, laboratory access, 156**
- Silk Road, The, 538–549, 563**
 - Dark Web investigations, 187
 - Hansa, 188
 - trial, 33
- SIM card readers, 139–140**
- SIM cards, 381–382, 419**
 - accessing, 388
 - cloning, 388
 - file systems, 386–387
 - forensics, 385–388
 - hardware, 386
 - interface, 386
 - iPhone, 513
 - PUC, 388, 419
- Simmonds, Jamie, 583**
- SIP (Session Initiation Protocol), network forensics, 348**
- Sixth Amendment (U.S. Constitution), 280–281, 306**
- skimmers, 8, 30, 166**
 - ATM skimmers, 166–167, 171
 - magstripe readers, 166–167, 172
 - parasites, 166, 172
- Skipeace, finding personal information, 194**
- Skype, 200, 453–455**
- SkyWave Mobile Communications, 410**
- slack (file), 37, 46**
- sleepimage files (macOS), 501, 534**
- Sleuth Kit (TSK), The, 144**
- small claims courts, 258, 309**
- SMART files, 150, 172**
- smart holster sensors, 584, 589**
- SmartCarving, 153**
- SmartMedia cards, 108**
- Smith v. Maryland, 442 U.S. 735 (1979), 272–273***
- SMS (Short Message Service), 388–389, 419**
- SMTP servers, 366**
 - email, 325–326
 - network forensics, 324–325
- Smyth v. The Pillsbury Company, 282***
- SnapChat, 466**
- snapshots (APFS), 493, 534**
- sniffers (packet), 316, 366**
- Snipping tool (Windows 10), 213**
- Snowden, Edward, 20**
- Snyder v. Phelps, 562 U.S. 443 (2011), 263***
- social networking**
 - background searches, 195–196, 202–205
 - Facebook, 203–204
 - geodata, 202–203
 - HootSuite, 196
 - MySpace, 205
 - online crime, 211–212
 - photo forensics, 461–462
 - Social Searcher, 196
 - Twitter
 - analytics, 204–205
 - API, 204
 - background searches, 204–205
 - Foller.me, 205
 - U.S. Department of Defense, 212
- Social Searcher, 196**

- sockpuppets, 178**
- soft/hard handoffs, 377, 418, 420**
- software, forensic imaging, 36**
- Sony Computer Entertainment America v. George Hotz, 287***
- Sony Music Entertainment v. Does, 326 F.Supp.2d 556, 565 (S.D.N.Y. 2004), 287***
- Sony PlayStation, 2011 breach, 314**
- SOP, cellphone forensics, 401–406**
- South Dakota v. Opperman (1976) 428 U.S. 364 [96 S.Ct. 3092],277***
- Souza, Dawnmarie, 176–177**
- space sharing (APFS), 492, 534**
- sparse bundles, 534**
- sparse images, 534**
- spindles, 37–38**
- spoilation of evidence, 12, 30**
- Spokeo, finding personal information, 194**
- Spotlight feature (macOS), 494, 534**
- Spy Dialer, 182–183**
- SQLite database, 420**
 - applications (apps), investigating, 427–431
 - Cache.db, 505
 - Mac forensics, 501
 - Tinder SQLite database, 427–429
- SSD (Solid State Drives), 101–103, 122**
 - FTL, 103, 121
 - garbage collection, 102, 103, 121
 - TRIM function, 103, 122
 - write-blockers, 109, 112
- standby council, 564**
- standing warrants, 271, 309**
- start screen, Windows 8.1, 79–80**
- state courts, 257**
 - appellate courts, 257
 - family courts, 258, 307
 - intermediate appellate courts, 257
 - juvenile courts, 258, 308
 - municipal courts, 258, 308
 - New York Trial Courts, 258–259
 - probate courts, 258, 309
 - small claims courts 258, 309
 - traffic courts, 258, 309
 - trial courts of general jurisdiction, 258–259
 - trial courts of limited jurisdiction, 258
- State of Connecticut v. John Kaminski, 115, 292–293***
- State v. Armstead, 292***
- stateful inspection firewalls, 339–340**
- stateless firewalls, 339–340**
- static analysis of applications (apps), SQLite database, 427–431**
- statistics, websites, 190–191**
- Statutory law, 254, 309**
- steganalysis, 168, 172**
- steganography, 168–169, 172**
- Stengart v. Loving Care Agency, Inc.6***
- Sticky Notes (Windows 7), 74–75**
- sting operations, 178**
- Stingray, 272, 309**
- STIX, 349**
- stolen property, searching for, 196–197**
- storage**
 - allocated storage space, 35–36
 - BD, 115–116, 120
 - CD, 113–114, 120
 - lands, 113–114, 121
 - pits, 113–114, 121
 - sessions, 114, 115, 122
 - TOC, 114, 122
 - tracks, 36, 114, 122
 - CD-RW, 114–115
 - DVD, 115, 120
 - file storage
 - 800-byte files, physical layout, 37
 - bytes, 36, 38–39

- clusters, 36
 - file slack, 37, 46
 - logical file size, 36
 - physical file size, 36
 - sectors, 36
 - tracks (CD), 36, 114, 122
 - floppy disks, 116–118, 121
 - hard disks
 - actuator arms, 37–38
 - cylinders, 38
 - determining capacity of, 38
 - disk geometry, 38
 - layout of, 37–38
 - page files, 39
 - Pagefile.sys, 39–42
 - platters, 37–38
 - spindles, 37–38
 - magnetic tapes, 114–115, 121
 - sectors, bad sectors, 36
 - unallocated storage space, 35–36
 - wear-leveling, 102, 122
 - zip disks, 118, 122
 - Strava application (app), 579–580**
 - structure of, comprehensive reports, 238–242**
 - STUN (Simple Traversal of UDP through NAT), network forensics, 348**
 - subnet masks, 321, 332, 366**
 - calculating, 334–335
 - Class A networks, 332
 - Class B networks, 332
 - Class C networks, 332
 - finding, 335
 - network forensics, 332–337
 - network masks, 333–334
 - reserved IP addresses, 334
 - subpoenas, 309**
 - subscribers (cellular networks)**
 - authentication, 382–383
 - records, 377–378, 420
 - subsidy locks, 379, 420**
 - Superfetch files, 58**
 - Supreme Court, The, 256**
 - surveillance**
 - online investigations, 177–178
 - search warrants, 272–273
 - video, 8
 - suspects, locating, 207**
 - svc.host.eve, IOC, 354**
 - SWDGE (Scientific Working Group on Digital Evidence), 129–130, 172, 470**
 - SWGIT (Scientific Working Group on Imaging Technologies), 471, 475**
 - switches, 324, 367**
 - Symbian OS, 400, 420**
 - SYN Flood attacks, 344**
 - SYN-SYN-ACK (TCP three-way handshake), 343**
 - System Restore, 71**
 - System Software Personalization (Apple), 508, 534**
 - System Status application (app), 235**
 - System32, IOC, 355**
 - Systrom, Kevin, 466**
-
- ## T
- T2 security chip (Apple), 492**
 - table of contents (ToC), reports, 239**
 - tablets, 413**
 - TAC (Type Allocation Codes), 378, 420**
 - tagged evidence, documenting, 229**
 - tags (macOS), 504, 534**
 - Tails, 185, 218**
 - TALON (Threat And Local Observation Notice), 209, 218**
 - tampering with evidence, 6, 30**
 - Target Disk Mode (macOS), 506–507**

taxes, virtual currencies, 188

TAXII, 349

TCP (Transmission Control Protocol), 343, 367

importance of, 344

retransmission, 344

TCP/IP headers, 344

three-way handshake, 343–344

TDMA (Time Division Multiple Access), 384, 420

tech forums, Intrusion Kill Chains, 351

Telegram, background searches, 195–196

telematics, 585, 589

telephone carriers, masking identities, 183

Ten Most Wanted list (FBI), 460

Terminal Window, 500

threats

APT, 314–315

botnets, 577

cryptojacking, 577–578, 588

malware, VPN, 178

MITM attacks, 433, 457

network attacks, investigating, 357

AmCache, 357–358

EDR, 359

Kibana, 359

Log2Timeline, 359

RAM, 357

SANS SIFT workstation, 360–361

ShellBags, 358

ShimCache, 358

VSC, 358

Windows Registry, 361–363

Trojan horses, 210, 218, 367

zero-day exploits, 426, 457

Zeus, 210, 218

three-way handshake (TCP), 343

TIFF files, 469, 475

Time Capsule (Airport), 488, 531

time zones, documenting investigations, 236

GMT, 237–238, 246

MST, 237, 246

UTC, 237, 246

times and dates

Epoch time, 496–497

HFS+490

timestamps

NTFS, 52

timestomping, 350, 367

Tinder application (app), 442–445

Tinder SQLite database, 427–429

Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969), 263–264

TLO (Terrorism Liaison Officers), 208–209, 218

TMSI (Temporary Mobile Subscriber Identities), 382, 386–387, 420

tmutil snapshot [enter],493

Tobolski, Donny, 177

TOC (Table of Contents)

CD, 114, 122

reports, 239

toolkits, 141

tools

documenting investigations, 234–236

network forensics, 315–316

TopSites.plist, 506

Tor, 184–185, 218

Touch ID (iPhone), 515–516, 534

touchscreen computing, Windows 7, 74

TPPO (Triphenylphosphine Oxide), 586, 589

Traceroute, 328, 367

track logs, GPS devices, 414, 420

trackpoints, GPS devices, 414, 420

tracks (CD), 36, 114, 122

traffic courts, 258, 309**traffic stops, search warrants, 277***Arizona v. Gant*, 278*California v. Nottoli*, 277–278*Carpenter v. United States*, 278–279*New York v. Perez* (2011 NY Slip Op 07659), 278*People v Spinelli*, 35 NY2d 77, 81, 278*South Dakota v. Opperman* (1976) 428 U.S. 364 [96 S.Ct. 3092], 277**training/education, 21**

colleges/universities, 22

high schools, 22

law enforcement, 21–22

professional certifications, 22–26

Transfer of Evidence, 4**Transport Layer (Layer 4), OSI model**

SYN Flood attacks, 344

TCP, 343

importance of, 344

retransmission, 344

TCP/IP headers, 344

three-way handshake, 343

UDP, 343

trials

criminal defense, 293

CCPA, 294

defense attorneys, 293–294, 307

NYS DFS Rule 23 NYCRR 500, 294–295

PIPEDA, 295

criminal trials versus civil trials, 261–262

expert witnesses, preparing, 243–244

Discovery phase, 290–291, 307

trial courts

of general jurisdiction, 258–259

of limited jurisdiction, 258

tricking, 558, 564**TRIM function, 103, 122****Tripp, Linda, 183****Trojan horses, 210, 218, 367****TSK (The Sleuth Kit), 144****TTP (Tactics, Techniques and Procedures),
Intrusion Kill Chains, 352–353****tumbcache.db, 469****Twitter**

analytics, 204–205

API, 204

background searches, 204–205

Foller.me, 205

U**Uber application (app), 451–453****UDID (Unique Device Identifiers), 509, 534****UDP (User Datagram Protocol), 343, 348, 367****UEFI (Unified Extensible Firmware Interface),
48****UICC (Universal Integrated Circuit Cards),
379, 420****U.K. (United Kingdom). See also E.U.**

U.K. Code of Practice for Consumer Internet of Things Security, 573

UK Modern Slavery Act, 301

Ulbrecht, Ross, 538–549, 563**UltraBlock Forensic Card Reader and Writer,
111–112****UMTS (Universal Mobile Telecommunications
System)), 385, 420****unallocated storage space, 35–36****undercover investigations, 218**

anonymity, 181–184

background searches, 177

email accounts, generating, 179–181

identities, generating, 178–179

sting operations, 178

surveillance, 177–178

warrants, 178

wiretaps, 178, 183

Unicode, 47

universities/colleges, digital forensic training, 22

UNIX, dd command, 119, 120, 157–158

upgrades, DFU Mode (iPhone), 512–513

UPS (Uninterruptible Power Supplies), 153, 172

URI (Uniform Resource Identifiers), 318, 367

URL Initiative (NCMEC), 462–463

U.S. Constitution, 254

Fifth Amendment, 279–280

First Amendment (U.S. Constitution), 262–263

Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008), 265

Internet and, 263–265

Layschock et al v. Hermitage School District et al, 264–265

Miller v. California, 413 U.S. 15 (1973), 265

Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969), 263–264

Fourth Amendment, 265–266

certiorari, 266, 306

exclusionary rule, 266, 307

fruit of the poisonous tree, 266, 278, 308

Katz v. United States, 389 U.S. 347 (1967), 266

O'Connor v. Ortega, 480 U.S. 709 (1987), 266

Olmstead v. United States, 277 U.S. 438 (1928), 266

search warrants, 266

warrantless searches, 268–271

Weeks v. United States, 232 U.S. 383 (1914), 266

Sixth Amendment, 280–281, 306

Supreme Court, The, 256

U.S. Department of Defense, social networking, 212

U.S. Department of Justice (NIJ)

cellphone forensics, 402–403

crime scenes, documenting, 226–227

U.S. District Courts, 257

U.S. DOJ (Department of Justice), warrantless searches, 268

U.S. legal system, 252, 254–255

admissibility of evidence, 262

Constitutional law, 262

First Amendment (U.S. Constitution), 262–265

Fourth Amendment (U.S. Constitution), 265–279

appeals courts, 255–256

Articles of the Constitution, 254

Bill of Rights, The, 254, 262, 306

burden of proof, 260–261, 306

Civil law, 254, 306

Codified law, 254, 306

common law, 254, 306

Constitutional law, 254, 262, 306

criminal defense, 293

CCPA, 294

defense attorneys, 293–294, 307

NYS DFS Rule 23 NYCRR 500, 294–295

PIPEDA, 295

criminal trials versus civil trials, 261–262

cross-examination, 260–261, 307

defendants, 253, 307

deliberations, 261, 307

direct examination, 260–261, 307

en banc, 561, 563

federal courts

appellate courts, 256–257

jurisdiction, 256

Supreme Court, The, 256

U.S. District Courts, 257

felonies, 261, 307

history of, 253–254

- judges, 255, 308
- juries, 260, 308
 - contempt of court, 260
 - foreperson, 260, 307
 - grand juries, 308
 - hung juries, 261, 308
 - indictments, 308
 - sequestration, 260, 308
 - voir dire, 260, 309
- Louisiana Civil Code Digest of 1808, 254
- misdemeanors, 261, 308
- Napoleonic Code, The, 254
- opening statements, 260–261
- origins of, 254
- plaintiffs, 130, 172, 253, 309
- precedents, 254, 309
- pro se, 552
- procedural overview, 259–260
- Regulatory law, 254, 309
- Roman law, 254
- standby council, 564
- state courts, 257
 - appellate courts, 257
 - family courts, 258, 307
 - intermediate appellate courts, 257
 - juvenile courts, 258, 308
 - municipal courts, 258, 308
 - New York Trial Courts, 258–259
 - probate courts, 258, 309
 - small claims courts, 258, 309
 - traffic courts, 258, 309
 - trial courts of general jurisdiction, 258–259
 - trial courts of limited jurisdiction, 258
- Statutory law, 254, 309
- structure of, 253–254
- subpoenas, 309
- UNITED STATES of America, Plaintiff-Appellee, v. Russell Lane WALSER, Defendant-Appellant. No. 01–8019, 269–270*
- United States v. Carey, No. 14–50222 (9th Cir. 2016), 269, 270*
- United States v. Daniel David Rigmaiden, 844 F.Supp.2d 982 (2012), 272–273*
- United States v. Dunn, 480 U.S. 294 (1987), 273*
- United States v. Jones, 274–276*
- United States v. Knotts 460 U.S. 276 (1983), 273–274*
- United States v. Leon, 468 U.S. 897 (1984), 267*
- United States v. Magana, 512 F.2d 1169, 1171 [9th Cir. 1975], 274*
- United States v. Mann (No. 08–3041), 270–271*
- United States v. McIver, 274*
- United States v. McConney, 728 F.2d 1195, 1199 (9th Cir.), 268*
- United States v. Tank, 292*
- United States v. Warsbak, 562 F. Supp. 2d 986 (S.D. Ohio 2008), 267*
- United States v. Ziegler, 267*
- U.S. Constitution, 254, 256
- verdicts, 261
- US Search, finding personal information, 192–193**
- USA PATRIOT Act (H.R. 3162), 14, 16–17, 268, 283, 284–286**
- USB devices**
 - debugging, 398, 420
 - flash drives, 106, 146–149
 - ownership, 72–73
- USB Restricted Mode (Apple), 510, 534**
- USBDeview, 72–73**
- usenet groups, 200–201, 218**
- user events (iPhone), 525**
- user groups, background searches, 196**
- user keybags, 492**

UserAssist, IOC, 357

\$USN_Journal, IOC, 355

USSS (United States Secret Service), history of digital forensics, 16–17

UTC (Coordinated Universal Time), 237, 246

UTM (Unified Threat Management), 339–340

V

vacuuming, 501, 534

vBulletin, background searches, 195–196

vector graphics, 468, 475

vehicle forensics

dogs, 586–587

VIN, 585–586, 589

VEK (Volume Encryption Keys), 491, 534

Venmo, 189

verdicts, 261

Vicemo, 189

video

Autopsy Video Triage, 213

capturing, 213–214

evidence

CCTV, 8–9

skimmers, 8

surveillance video, 8

websites visited/Internet searches, 9

Real Player, 214

SaveVid.org, 213

WM Recorder, 214

viewing

BIOS, 48–49

cookies, 214

websites visited, 215

VIN (Vehicle Identification Numbers), 585–586, 589

Virginia Declaration of Rights, 262

virtual assistants

Alexa, 191, 578–579

Cortana, 82–83

virtual currencies

Bitcoin, 188, 216

Bitcoin miners, 189, 216

Bitcoin tumblers, 189, 216

Bitcoin wallets, 188–189, 216

blockchains, 189, 217

identities, generating, 178

CoinMarketCap, 188

cryptojacking, 577–578, 588

Fiat currency, 188, 217

FinCEN, 188

history of digital forensics, 20

identities, generating, 178

IRS, 188

Linden dollars, 188

taxes, 188

Venmo, 189

Vicemo, 189

virtual memory, 39, 42

visited websites/Internet searches, 9

Vista, 63, 68

defragmentation, 63–64

Event Viewer, 65–66

Hyberfil.sys, 68

metadata, 67

physical memory, 67

ReadyBoost, 67

Volume Shadow Copy Service, 67–68

Windows search engine (indexing), 66

VLR (Visitor Location Register), 382, 420

VM (Virtual Machines), 150–151- 151, 172

VMware, 151

Vo5G wireless standard, 575, 589

VoIP (Voice over Internet Protocol), 367

network forensics, 345–346

STUN, 348

voir dire, 260, 309

volume headers, 489–490, 534

Volume Keybags, 491, 534

Volume Shadow Copy Service, 67–68

VPN (Virtual Private Networks), 178

VSC (Volume Shadow Copy), 358

W

War Games, 15

warrants,

search warrants

court orders, 272, 307

digital surveillance, 272–273

email, 267

GPS tracking, 273–276

MLB and BALCO, 268

pen registers, 272–273, 308

probable cause, 267, 309

Smith v. Maryland, 442 U.S. 735 (1979), 272–273

traffic stops, 277–279

United States v. Daniel David Rigmaiden, 844 F.Supp.2d 982 (2012), 272–273

United States v. Leon, 468 U.S. 897 (1984), 267

United States v. Warshak, 562 F. Supp. 2d 986 (S.D. Ohio 2008), 267

United States v. Ziegler, 267

standing warrants, 271, 309

warrantless searches, 269

Arizona v. Gant, 2009, 271

case studies, 271

DOJ, 268

exigent circumstances, 268, 307

Horton v. California, 269

"knock and talk" 269, 308

People v. Diaz, 271

plain error, 270, 308

plain view doctrine, 269, 308

Riley v. California, 271

Rules of Criminal Procedure, 270, 309

search incident to a lawful arrest, 271

standing warrants, 271

United States of America, Plaintiff-Appellee, v. Russell Lane WALSER, Defendant-Appellant. No. 01–8019, 269–270

United States v. Carey, No. 14–50222 (9th Cir. 2016), 269, 270

United States v. Mann (No. 08–3041), 270–271

United States v. McConney, 728 F.2d 1195, 1199 (9th Cir.), 268

Washington v. Jackson, 150 Wash.2d 251, 76 P.3d 217 (Wash. 2003), 276

WayBackMachine, 189–190

waypoints, GPS devices, 414, 420

W-CDMA (Wide Band CDMA), 384, 420

WD (Western Digital) external hard drives, 107

weaponization (Intrusion Kill Chains), 352

wear-leveling, 102, 122

web browsers, 367

Edge web browser, 82

viewing websites visited, 215

WebCacheV01.dat, 215, 218

InPrivate Browsing, Internet Explorer, 76–77

network forensics, 318–319

Safari, 504

Cache.db, 505

Cookies.plist, 505

Downloads.plist, 505

History.plist, 504–505

iPhone, 518

TopSites.plist, 506

webpage reviews, 504–505

for Windows, 506

Windows 7, 76–77

web hosting, 132

web servers, 9, 30, 367

- network forensics, 317–321
 - HTTP, 319–320
 - scripting languages, 320–321
 - URI, 318
- web browsers, 318–319
- web browsers, network forensics, 318–319, 367

WebCacheV01.dat, 215, 218**webpage reviews, Safari web browser, 504–505****websites**

- archives, 189–190
- background searches
 - professional networks, 205–206
 - social networking websites, 202–205
- evidence, 189
 - website archives, 189–190
 - website statistics, 190–191
- IsAnybodyDown website, photo forensics, 464
- statistics, 190–191
- TopSites.plist, 506
- websites visited/Internet searches, 9

Weeks v. United States*, 232 U.S. 383 (1914), 266**Wichita Eagle Newspaper*, 118****Wi-Fi**

- Apple devices, 487–488
- mesh networks, 576, 589
- Wi-Fi 6, 575–576, 589

Windows 7, 68

- backing up to networks, 71–72
- Backup and Restore Center, 68
- biometrics, 69
- BitLocker To Go, 72
- COFEE, 72
- Event Viewer, 76
- grouping files, 78
- InPrivate Browsing, 76–77

JumpLists, 69

- restoration points, 71
- Sticky Notes, 74–75
- System Restore, 71
- touchscreen computing, 74
- USB device ownership, 72–73
- web browsers, 76–77
- Windows Federated Search, 79
- Windows Registry
 - analysis, 75
 - registry paths and corresponding files, 76

Windows 8.1

- applications, 81
- desktop, 80–81
- evidence gathering, 81–82
- security, 82
- start screen, 79–80

Windows 10, 82

- Cortana, 82–83
- Edge web browser, 82
- notifications, 82
- screen captures, 213
- Snipping tool, 213

Windows 10 Mobile, 400, 420**Windows Federated Search, 79****Windows File Registry, 106****Windows file systems**

- defined, 49
- FAT, 464
 - defined, 50
 - FAT12, 50
 - FAT16, 50
 - FAT32, 50
 - FAT64, 50
 - FATX, 50
- feature comparisons table, 52
- NTFS, 51–52

- defined, 50
- FTK Imager, 53–56
- MFT, 52
 - system files, 53
- Prefetch files, 57, 355, 366
- ShellBags, 58
- ShimCache, 58–59
- Superfetch files, 58
- Windows Registry, 59–60, 61
 - analysis, Windows 7, 75
 - data types, 61
 - FTK Registry Viewer, 62
 - HKCC, 61
 - HKCR, 60
 - HKCU, 60–61
 - HKLM, 61
 - HKU, 61
 - Registry Editor, 60
 - registry paths and corresponding files, Windows 7, 76
- Windows OS**
 - Microsoft Office, 62–63
 - Microsoft Office 365, 83
 - Safari web browser, 506
 - subnet masks, finding, 335
 - tumbcache.db, 469
 - Vista, 63, 68
 - defragmentation, 63–64
 - Event Viewer, 65–66
 - Hyberfil.sys, 68
 - metadata, 67
 - ReadyBoost, 67
 - Volume Shadow Copy Service, 67–68
 - Windows search engine (indexing), 66
 - Windows 7, 68
 - backing up to networks, 71–72
 - Backup and Restore Center, 68
 - biometrics, 69
 - BitLocker To Go, 72
 - COFEE, 72
 - Event Viewer, 76
 - grouping files, 78
 - InPrivate Browsing, 76–77
 - JumpLists, 69
 - restoration points, 71
 - Sticky Notes, 74–75
 - System Restore, 71
 - touchscreen computing, 74
 - USB device ownership, 72–73
 - web browsers, 76–77
 - Windows Federated Search, 79
 - Windows Registry, 75–76
 - Windows 8.1
 - applications, 81
 - desktop, 80–81
 - evidence gathering, 81–82
 - security, 82
 - start screen, 79–80
 - Windows 10, 82
 - Cortana, 82–83
 - Edge web browser, 82
 - notifications, 82
- Windows Registry, 59–60, 61**
 - analysis, Windows 7, 75
 - data types, 61
 - FTK Registry Viewer, 62
 - HCR (HKEY_CURRENT_USER), 363
 - HCU (HKEY_CURRENT_CONFIG), 363
 - HKCC, 61
 - HKCR, 60
 - HKCR (HKEY_CLASSES_ROOT), 363
 - HKCU, 60–61
 - HKLM, 61, 363
 - HKU, 61
 - HKU (HKEY_USERS), 363

- Index.dat, 215, 217
 - network attacks, investigating, 361–363
 - Registry Editor, 60
 - registry paths and corresponding files, Windows 7, 76
 - websites visited, viewing, 215
 - Windows search engine (indexing), Vista, 66**
 - WinHex, 144**
 - Winslow II, Kelvin, 580**
 - wireless monitoring, applications (apps), 431–433**
 - wireless telecommunications technologies**
 - 3GP, 384–385, 416
 - 3GP2, 385, 416
 - 4G, 383
 - 4G LTE Advanced, 383, 416
 - 5G, 384, 573–575, 588
 - CDMA, 385, 417
 - CDMA2000, 385, 417
 - EDGE, 384–385, 417
 - GRPS, 384–385
 - GSM, 384, 418
 - iDEN, 385
 - MiFi, 383, 419
 - multiplexing, 385, 419
 - TDMA, 384, 420
 - UMTS, 385, 420
 - Vo5G, 575, 589
 - W-CDMA, 384, 420**
 - Wi-Fi 6, 575–576, 589
 - wiretaps, 178, 183**
 - witnesses**
 - depositions, 290, 307
 - expert witnesses, 242, 246, 290–291
 - goals of, 242
 - preparing for trial, 243–244
 - role of, 242
 - tips for prosecution, 244
 - lay witnesses, 243, 246
 - WM Recorder, 214**
 - Wolf, Miss Teen USA Cassidy, 464**
 - workbenches, 134, 172**
 - worksheets, documenting investigations**
 - computer worksheets, 230–231
 - hard disk drive worksheets, 232
 - server worksheets, 233–234
 - workstations, 133**
 - ergonomics, 154
 - FRED workstations, 153
 - SANS SIFT workstation, 360–361
 - write-blockers, 101, 107–108, 109, 112, 114, 122, 137–139**
 - WWW (World Wide Web), 184**
-
- X**
-
- xD Picture Cards, 111, 122**
 - XMPP (Extensible Messaging and Presence Protocol), 199, 217**
 - X-Ways Forensics software, 7, 144**
-
- Y**
-
- YARA, Intrusion Kill Chains, 353**
-
- Z**
-
- Zaba Search, finding personal information, 192**
 - zero-day exploits, 426, 457**
 - Zeus, 210, 218**
 - ZIF cables, SATA, 96–97**
 - zip disks, 118, 122**