PEARSON IT

CYBERSECURITY CURRICULUM

SECOND EDITION

A PRACTICAL GUIDE TO DIGITAL FORENSICS INVESTIGATIONS

DR. DARREN R. HAYES

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

ISBN-13: 978-0-7897-5991-7
ISBN-10: 0-7897-5991-8

Library of Congress Control Number: 2020906041

ScoutAutomatedPrintCode

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
Aamir 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 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 Technologies, Inc. All Rights Reserved
Figure 12-9	Screenshot of PMAP Info from BlackBag Technologies © 2020 BlackBag Technologies, 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	CKA /Shutterstock
“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.”	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.”	State v. Armstead, No. 82-KA- 0896, May 23, 1983.
regular practice of that business activity	Rule 803, Exceptions to the Rule Against Hearsay, Federal Rules of Evidence
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.	Rule 901, Requirement of Authentication or Identification, Federal Rules of Evidence
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.	John Adams, Second President of the United States (1797-1801).
§ 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	The New York State (NYS) Department of Financial Services (DFS), Section 500, 2017
§ 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.	Canada Personal Information Protection and Electronic Documents Act (PIPEDA), 2000
(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	Directive 95/46/EC of the European Parliament and of the Council
“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”	Article X, Federal Rules of Evidence (FRE), Rule 1001: Contents of Writings, Recordings and Photographs
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.	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://tydgccykixpbu6uz.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	Quoted by Ross William Ulbricht, American convict
"anybody know someone that works for UPS, FedEX, or DHL?"	Quoted by Ross William Ulbricht, American convict, April 2012
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://jhiwjjlqpyawmpjx.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://jhiwjjlqpyawmpjx.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	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 wich [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	United States District Court for the Eastern District of Virginia
[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.	United States v. Zacarias Moussaoui, Criminal No. 01-455-A, United States District Court, E.D. Virginia, Jun 18, 2002
"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."	United States v. Zacarias Moussaoui, Criminal No. 01-455-A, United States District Court, E.D. Virginia, Jun 18, 2002
"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."	U.S. Code Title 47. TELECOMMUNICATIONS. Section 223. Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications
"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."	State of New Jersey vs. Dharun Ravi, Supreme Court of New Jersey
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.	United States v. Comprehensive Drug Testing, Inc., United States Court of Appeals, 513 F.3d 1085 (9th Cir. 2008)
"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".	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 of 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

Table of Contents

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 must 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.

Aamir 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.

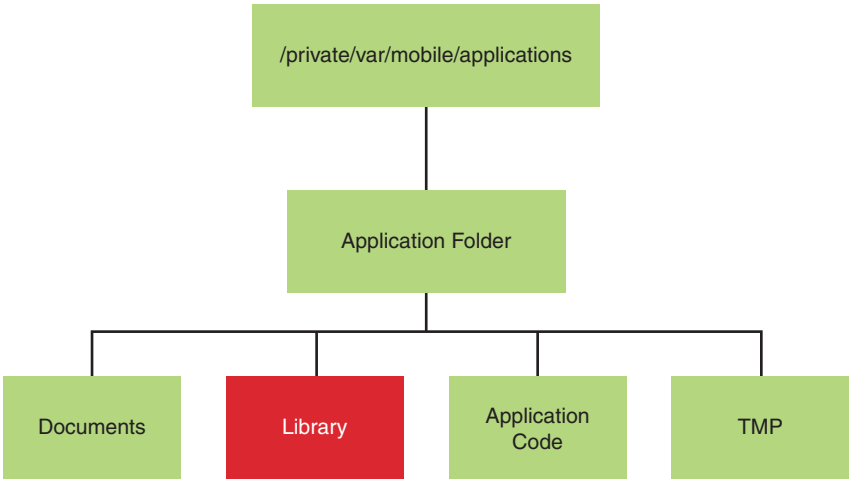
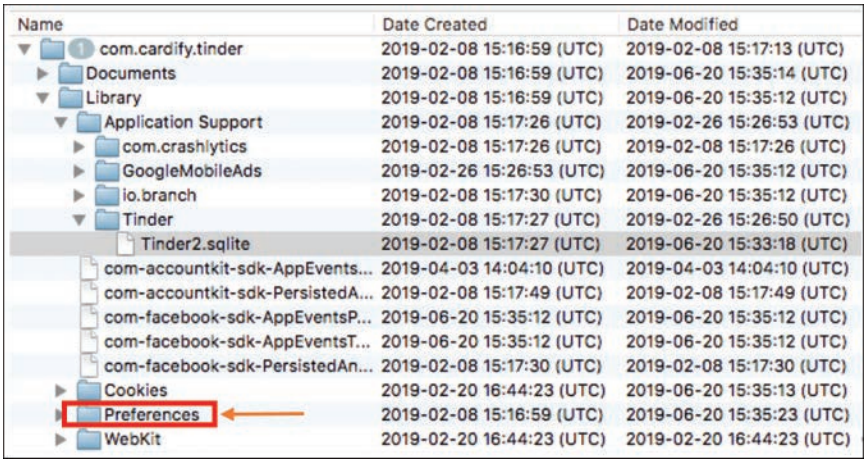


FIGURE 10.2 Application storage on iOS

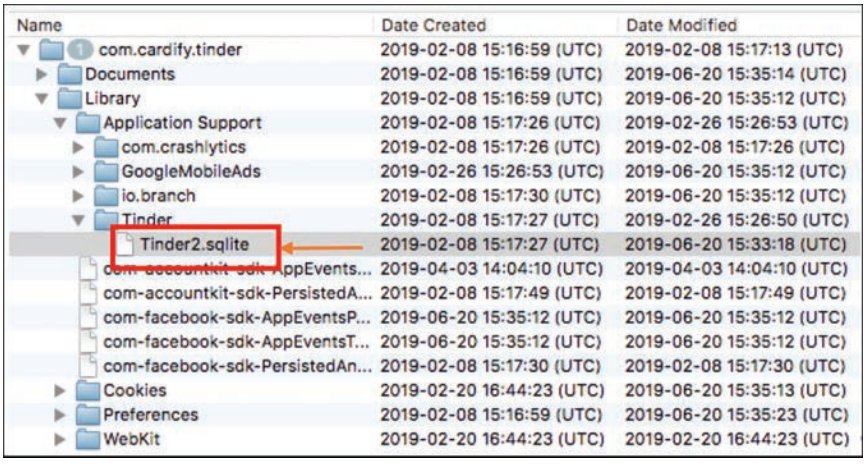
The `Library` folder, which is highlighted in Figure 10.2, is where you will find the all-important user data, including cache, cookies, and other personal information. In the `Preferences` folder, which is displayed and highlighted in Figure 10.3, you may actually discover usernames and passwords that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

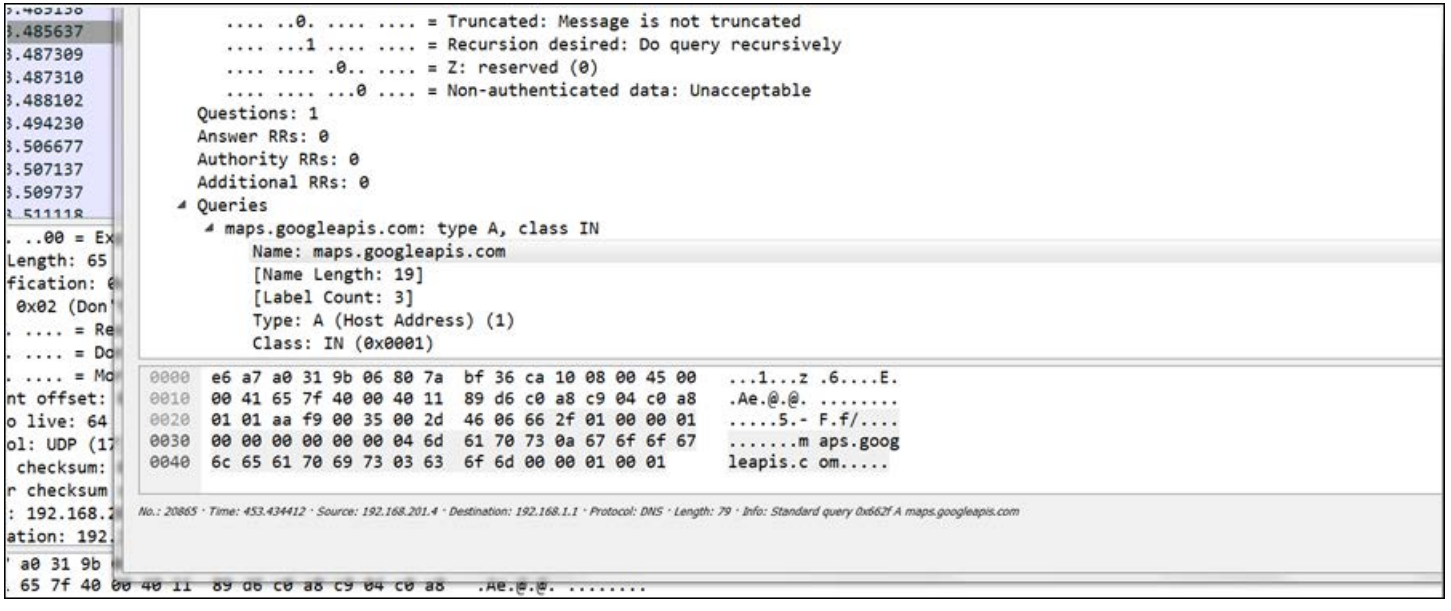


FIGURE 10.6 Google Maps API identified in a PCAP captured by Wireshark

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

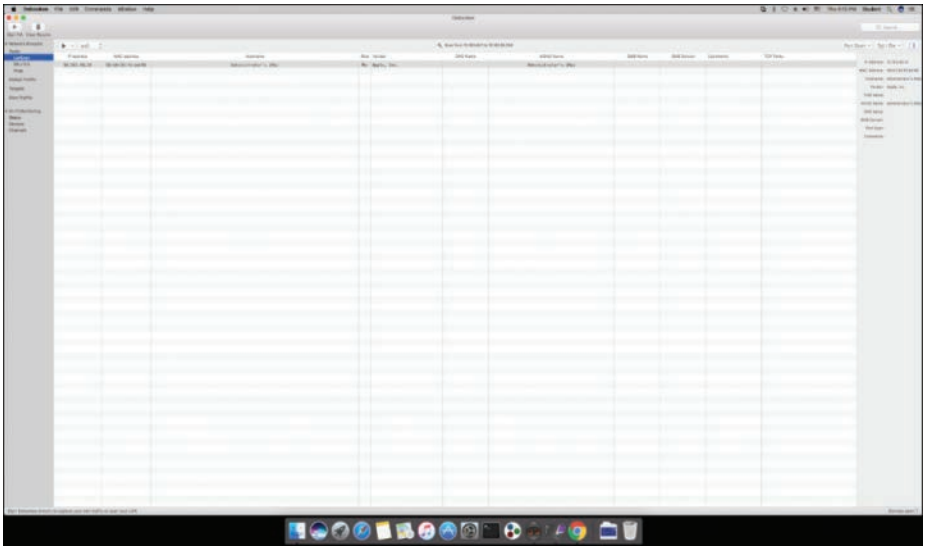


FIGURE 10.8 Debookee user interface

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.

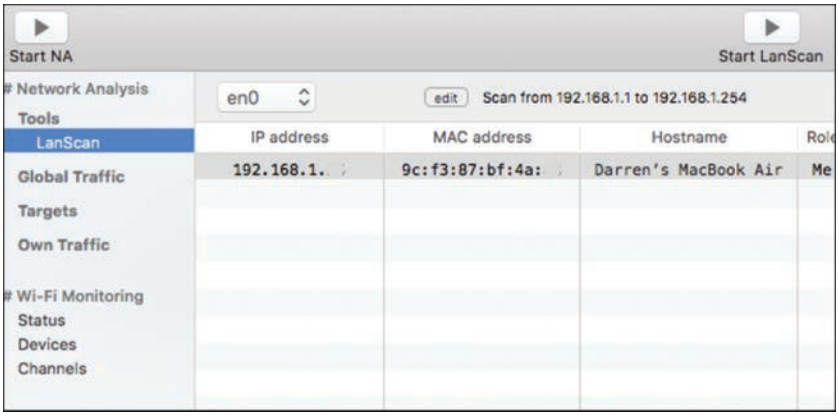


FIGURE 10.9 Debookee user interface with host computer information displayed

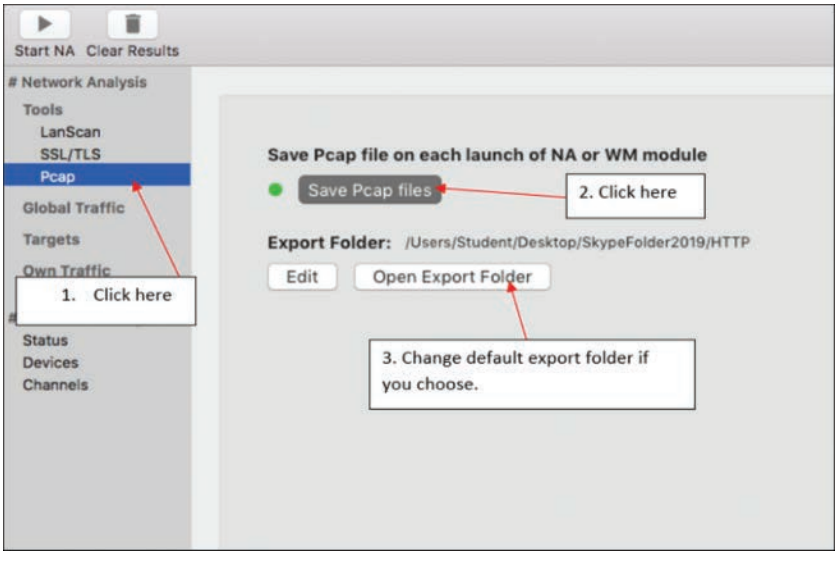


FIGURE 10.10 *Save Pcap files* option in Debookee

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.

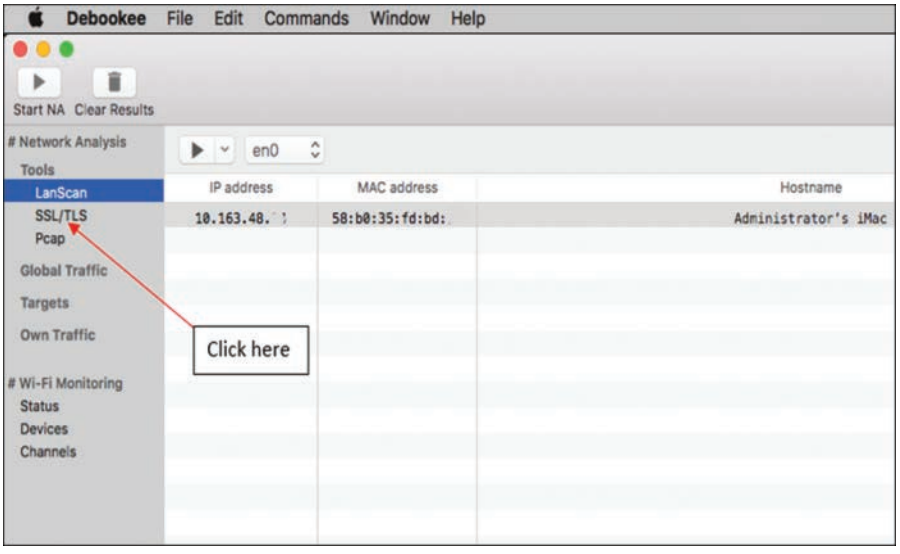


FIGURE 10.11 SSL/TLS decryption option in Debookee

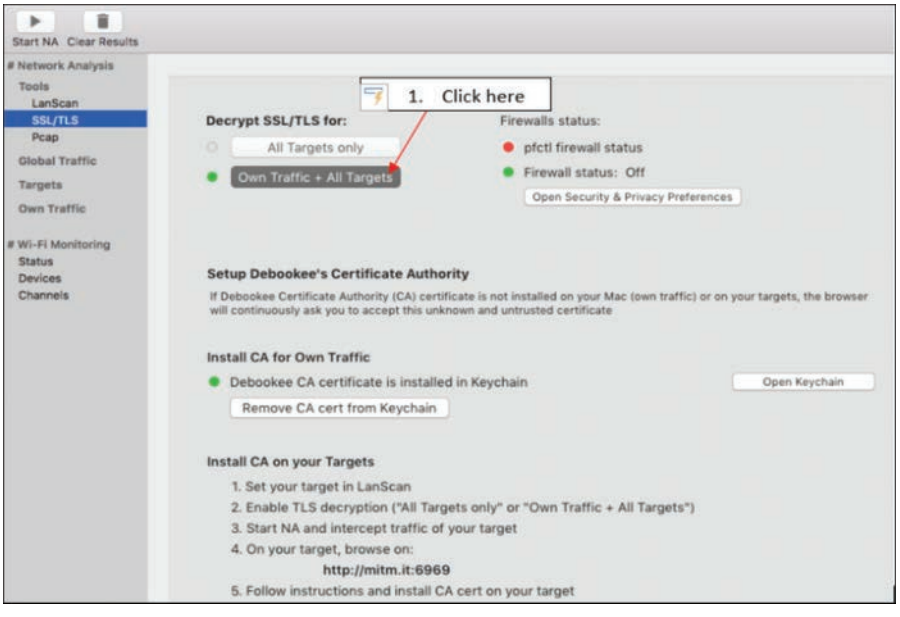


FIGURE 10.12 Decryption option in Debookee

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.

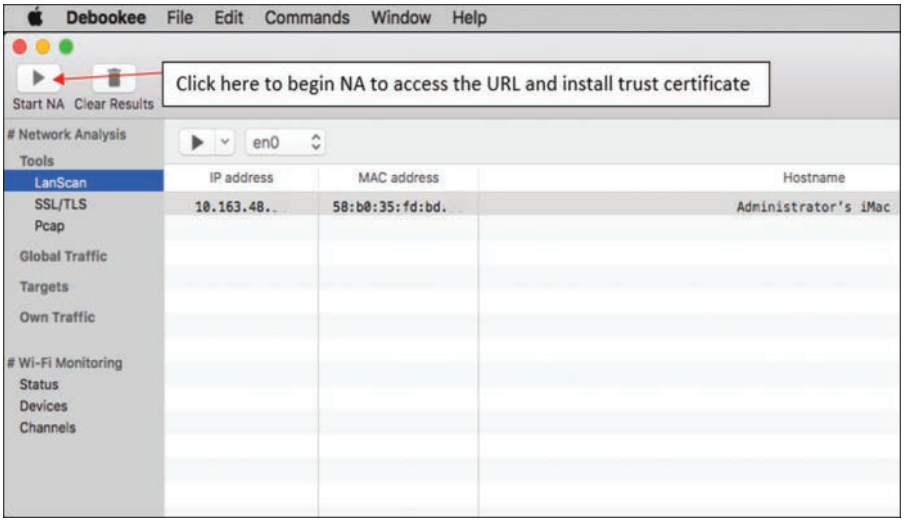


FIGURE 10.13 Start NA option in Debookee

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.robtex.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.

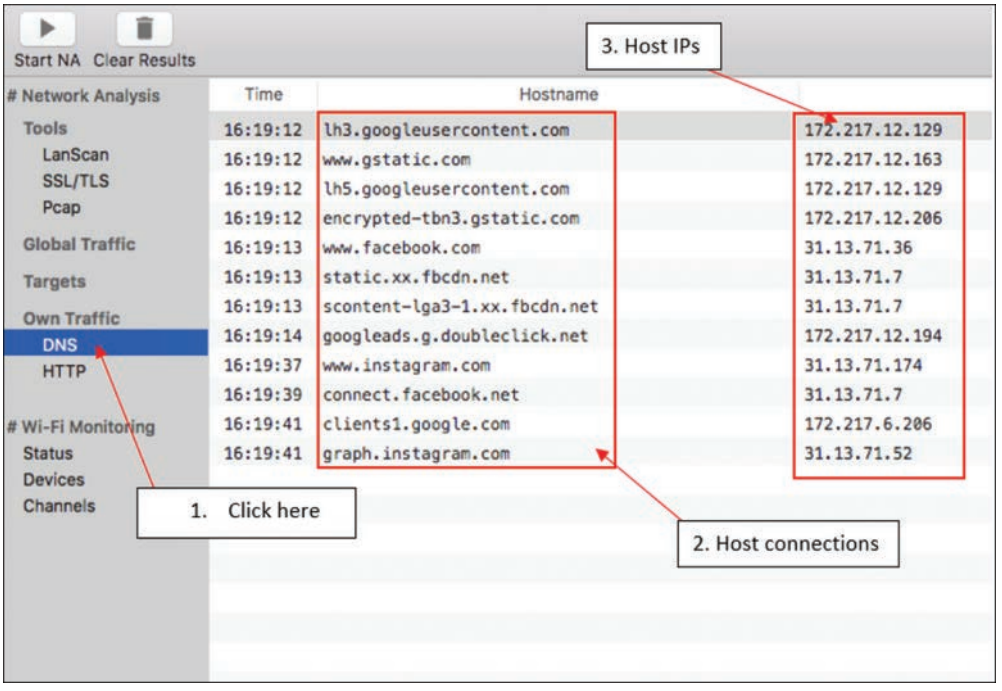


FIGURE 10.14 DNS connections captured

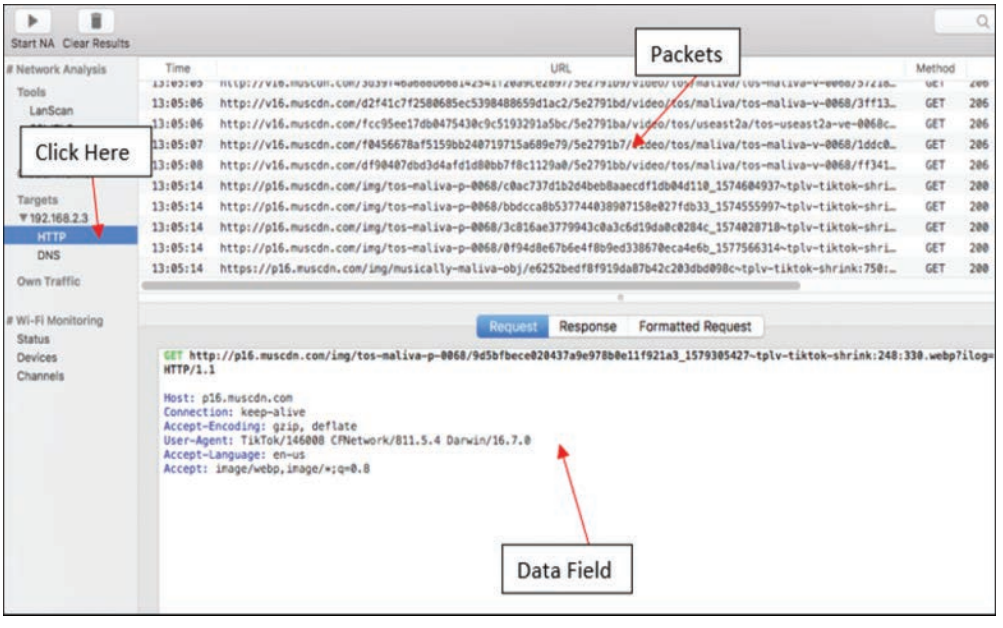


FIGURE 10.15 Decrypted TikTok packet (pcap)

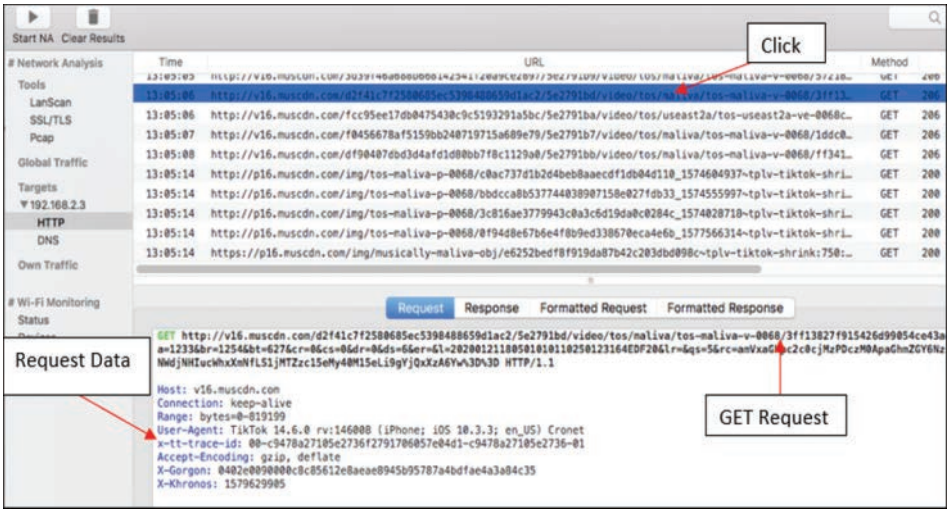


FIGURE 10.16 GET request data displayed

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.

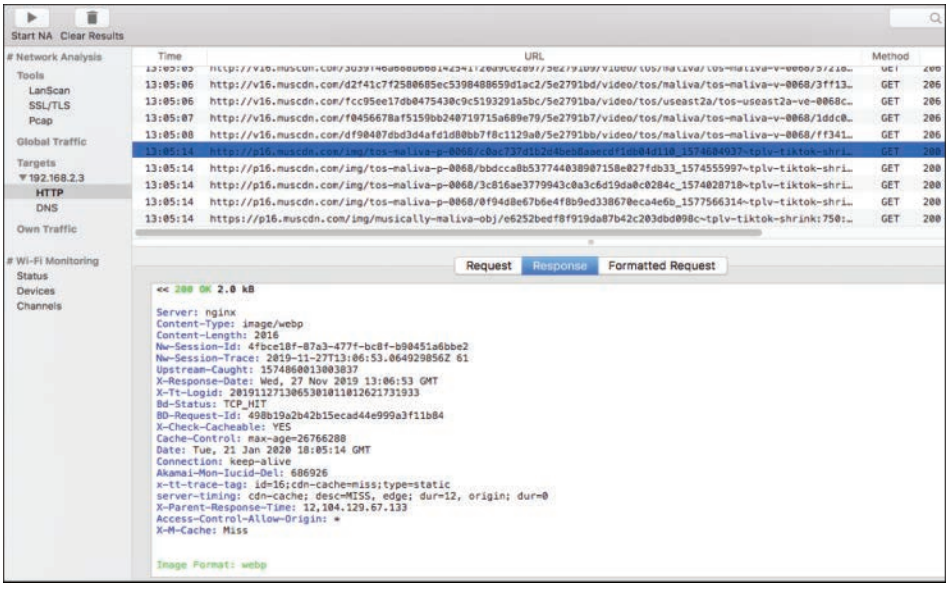


FIGURE 10.17 Response results

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.

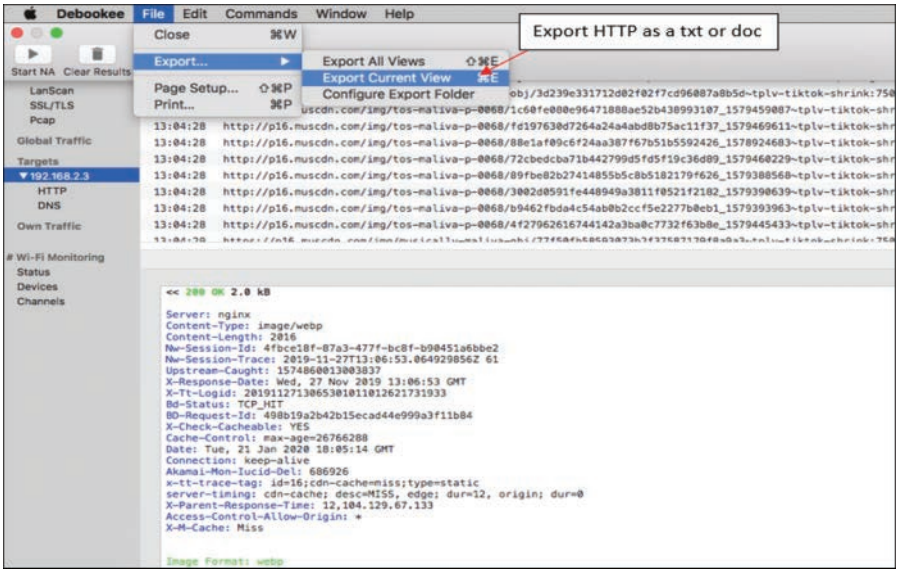


FIGURE 10.18 Data Export feature in Debookee

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

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.

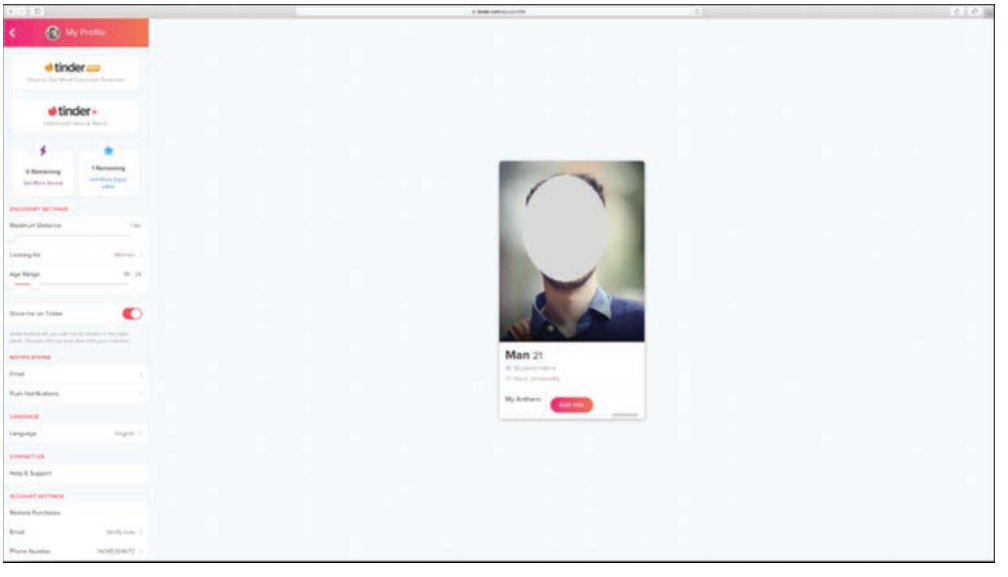


FIGURE 10.21 www.gotinder.com user profile

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".

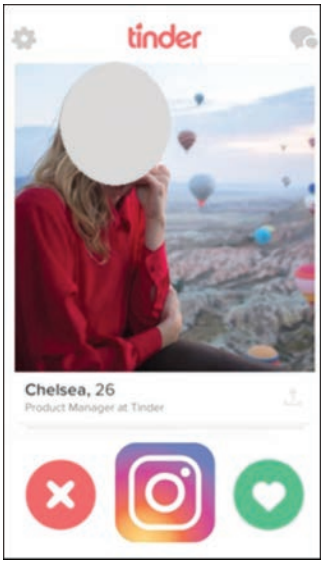


FIGURE 10.22 Tinder app linked to Instagram

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.

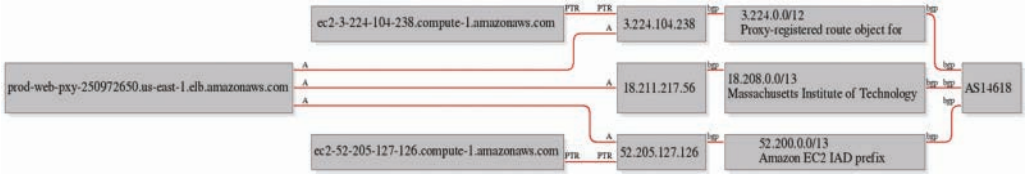


FIGURE 10.23 DNS data for gotinder.com (Source: Robtex.com)

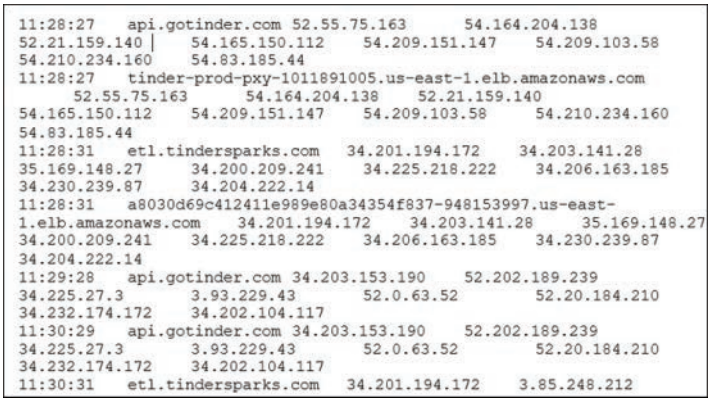
Utilizing tools, like Robtex and traceroute, and whatismyipaddress.com, an investigator can determine where app user data is being stored and determining jurisdiction.

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-CAFBFA75BE0F",
"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.

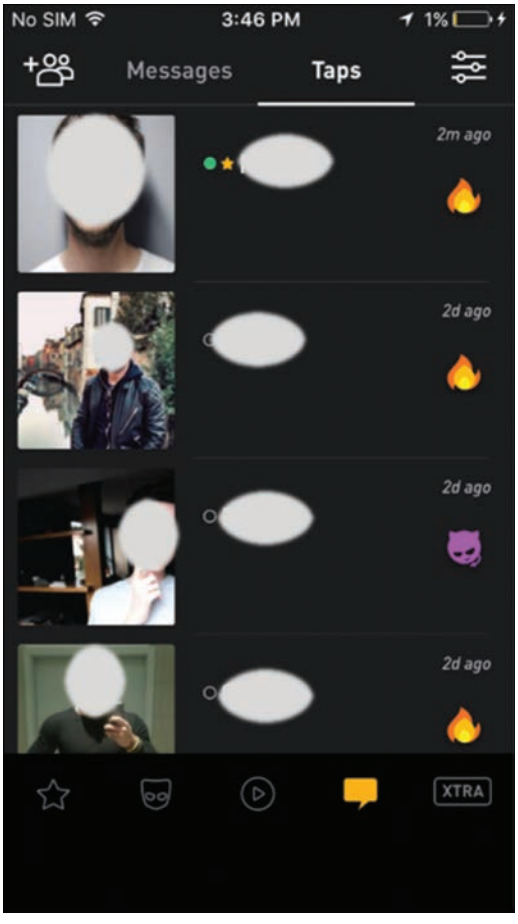


FIGURE 10.28 Grindr mobile user chat interface

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.

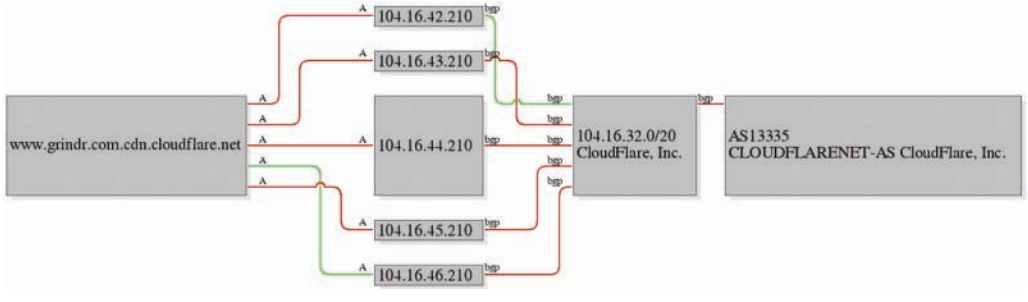


FIGURE 10.29 www.grindr.com.cdn.cloudfare.net DNS map (Source: Robtex.com)

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=d368ff8b86152eab3a1603d1f3c3a02511558628848;
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.

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

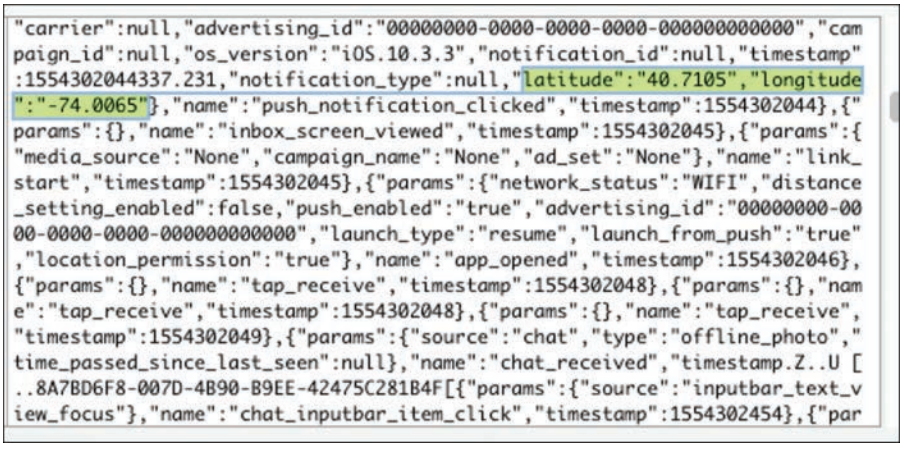


FIGURE 10.32 Latitude/longitude data from `greventLog.sqlite`

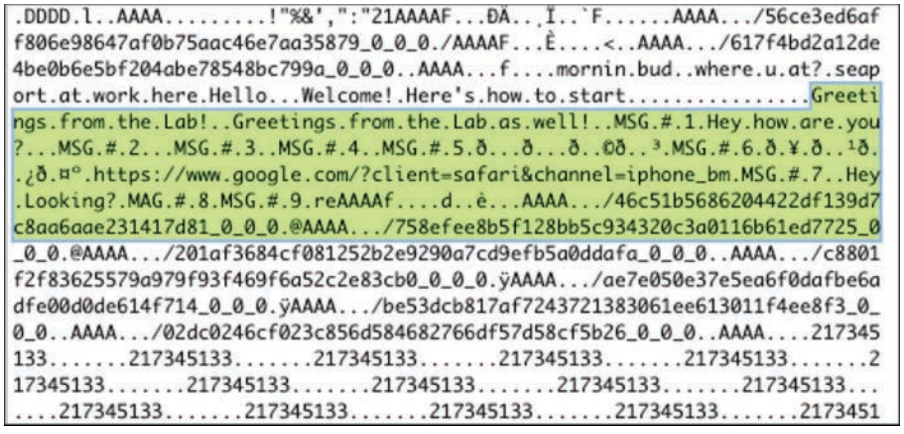


FIGURE 10.33 Text messages extracted in plaintext viewed in Hex Tab (BlackLight)

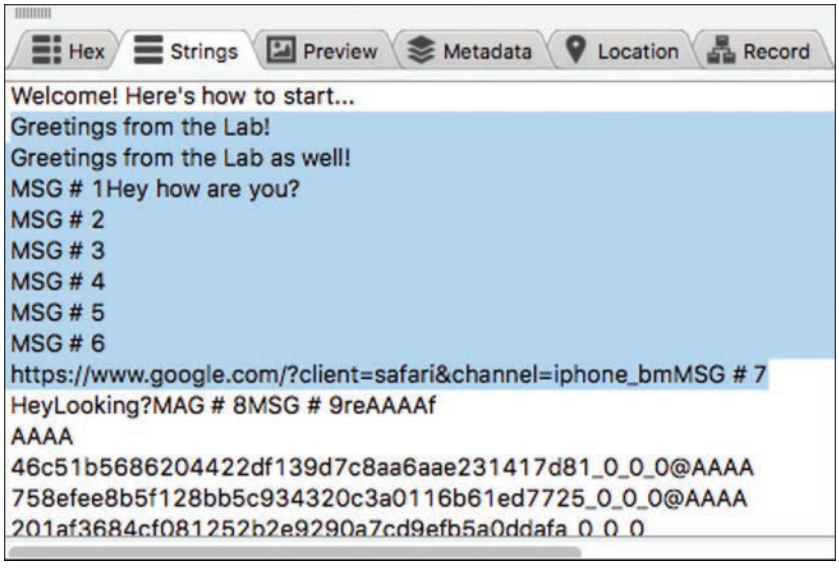


FIGURE 10.34 Text messages in plaintext viewed in Strings tab (BlackLight)

Rideshare Apps

Location information is always important in an investigation because an investigator does not just search for incriminating evidence but also needs to identify where a suspect was. As you will learn, rideshare apps, like Uber, contain extensive geolocation data that is easily accessible.

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.

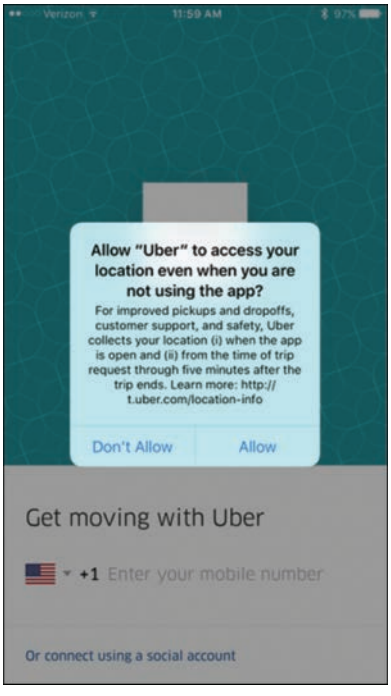


FIGURE 10.35 Uber dialog box during installation

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\<Skype Name>
```

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.

Index

Symbols

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z