C23 Darknet Investigation and Forensic Techniques

Sarah Cortes, PhD, Inman Technology, 899 Green Street, San Francisco, CA 94133*

After attending this presentation, attendees will be made aware of the utility of using darknet tools to conduct investigations. Attendees will be able to define the darknet in technical terms, know how to install darknet software in the lab, and be able to conduct a darknet investigation. Attendees will learn about recent darknet cases, and how investigators can make use of darknet tools to assist in their investigations.

This presentation will impact the forensic science community by increasing awareness of the darknet and the capabilities of darknet tools and investigative techniques. Further, this presentation will inform attendees regarding the use of darknet tools and investigative techniques in current cases, detailing results and conclusions as to effective techniques based on lab testing.

By reviewing several recent darknet operations, this presentation will explain how others have successfully employed digital and network evidence extraction techniques to investigate darknet cases and how one successful darknet case can jumpstart another. Understanding these darknet investigation techniques impacts the forensic science community by increasing investigator capabilities and options when facing darknet technology, illustrated by their use across several major cases.

The shutdown of online drug and contraband marketplaces AlphaBay and Hansa swept headlines in July 2017; however, prior to AlphaBay, Law Enforcement Agencies (LEAs) prevailed in a number of darknet cases. An increasing number of global darknet investigations have identified suspects and opened cases in jurisdictions across the United States, ultimately pushing arrests down to the state and local level. This presentation reviews darknet technology and techniques such as the ones deployed in these actual investigations.

In one case, unknown to the general public, in the predawn hours beginning April 4, 2015, in time zones across the world, LEAs in nearly every state in the United States and in 17 other countries started knocking on doors, surprising occupants, and handcuffing suspects in one of the most far-reaching child abuse darknet cases in history: Operation Pacifier. Over 200 prosecutions have followed in jurisdictions across the United States. Based on extensive appeals, some are still ongoing as of 2017. In the weeks that followed, defense attorneys, journalists, and the public wanted to know how investigators identified the defendants. This presentation reviews how darknet suspects may be deanonymized in theory and in actual cases.

The scale and scope of the recent and ongoing Operation Pacifier darknet cases is unprecedented. Globally, it encompasses more than 17 countries' Law Enforcement Agencies (LEAs), Europol, and, in the United States, the Federal Bureau of Investigation (FBI) and more than 200 cases in more than half of the United States state judicial systems. Operation Pacifier and other recent darknet cases, such as Silk Road and Operation Onymous, have raised myriad new technical issues, as well as legal issues and rule changes, across many jurisdictions.

While the darknet has a number of legitimate uses, it has also become a haven for criminals.[1-3] Investigators have been developing, refining, and implementing techniques to infiltrate the darknet and use them to solve cases involving narcotics trafficking, carding, identity theft, child abuse, and other illegal activities.[4-7]

Darknet cases and issues reflect that, as technology advances, so do criminal methods. Like a technological cat-and-mouse game, law enforcement has had to develop compensating online darknet tools and tactics. The darknet has spawned unique legal and technical issues, which has required a fundamental change in investigative ground rules, because it conceals suspects' identities by concealing their Internet Provider (IP) address. In order to attack and defeat darknet technology and its anonymity, LEAs have adapted, from use on the surface web, what are broadly called Network Investigative Techniques (NITs). NIT is a term covering a wide scope of investigative strategies, tools, and approaches, including scripts, server takeovers, or simply observing email header information.

Legally, NITs are generally used in searches and seizures of computers, devices, or other technology, which means they may fall under the scope of the Fourth Amendment. Because they are often performed blind with respect to the target's identity and therefore location, they can, and frequently do, involve criminal investigation searches outside the United States, including searches of non-United States citizens.

This study selected and reviewed eight related darknet investigative operations, including Operation DarkNet-Lolita City (2011), Operation TorPedo-PedoBoard (2011-13), Operation Freedom Hosting (2013), Operation Silk Road (2013), Operation Onymous-Silk Road 2.0 (2014), Task Force Argos KidClub (2014), Task Force Argos LoveZone (2014), and Operation Pacifier-Playpen (2014-15). Prosecutions in many of these cases are still ongoing today, as appeals reach higher courts and constitutional and other issues are adjudicated.

Darknet cases and evolving investigative techniques have also raised legal challenges.[8] These include Fourth Amendment search and seizure issues, challenges to the Fifth and Fourteenth Amendments, *Daubert*, and Rule 702 and evidence issues, NIT usage, the standards for scientific validity (to which the President's Council of Advisors on Science and Technology (PCAST) creates new perspective), Sixth Amendment discovery scope issues, and issues of international law, including the role of Mutual Legal Assistance Treaties (MLATs). How these issues have played out in actual prosecutions, as the law advances in response to technology innovations, are reviewed.

Reference(s):

1. Attorney General Jeff Sessions Delivers Remarks at Press Conference Announcing AlphaBay Takedown. US DOJ official website, July 20, 2017.
2. https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-delivers-remarks-press-conference-announcing-alphabay.
3. BBC News. *Sessions on dark web Alphabay and Hansa shut down.* July 20, 2017. http://www.bbc.com/news/av/technology-28591682/dark-net-drugs-adverts-double-in-less-than-a-year.

*Presenting Author

4. Lewman, A. Tor: Uses and Limitations of Online Anonymity. *Advances in cyber security: technology, operations, and experiences.* ed. DF Hsu, D Marinucci, Oxford University Press, 2013.

5. Lewman, A. The Internet and drug markets, EMCDDE Addiction. *European Monitoring Center for Drugs and Drug Addiction (EMCDDA)*. 1 (1), 11, 2015.

6. Owenson, G.H. and Savage, N.J. (2015). The Tor Darknet. *Global Commission on Internet Governance, 20.* https://www.ourinternet.org/research/tor-dark-net.

7. Sarah Cortes. MLAT World Treaty Cartel Internet Overlay for Digital Traffic Analytics for MLAT.is. *Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST17).* April 2017.

8. Cortes, S. (2015), Legalizing Domestic Surveillance: The Role of Mutual Legal Assistance Treaties in Deanonymizing TorBrowser Technology. In: *Richmond Journal of Law and Technology (JOLT).* 22 Rich. J.L. & Tech. 6.

Darknet, Tor, Network Forensics

*Presenting Author