Chapter 11

Connecting Related Online Elements with Maltego Carbon 3.5.3™:
Six Use Cases for Higher Education

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

With so much of modern life conducted in online spaces, understanding what is knowable through those spaces is a critical aspect of digital literacy and informational awareness. To increase online transparency, Maltego Carbon 3.5.3 (a penetration testing tool) enables powerful exploration of the Surface Web through its “machines” and “transforms.” Maltego enables the exploration of the interconnections between disparate pieces of online information (including technological understructures, documents, aliases, images, phrases, email addresses, telephone numbers, social media accounts, and geographical location coordinates. In the educational context, this tool may be applied in a number of ways. This chapter summarizes six generic “use cases”: Use Case 1: Understanding an Online / Offline Entity; Use Case 2: Exploring a Domain; Use Case 3: From Physical Location to Cyber and Back Again; Use Case 4: Online Conversations on Social Media Sites; Use Case 5: Eventgraphing: Mapping an Event Online, and Use Case 6: Finding Leads to Enhance Research.

INTRODUCTION

The World Wide Web and Internet have been compared to a large-scale database with heterogeneous data. To access the data contained in these online spaces, it is critical to have the appropriate tools. Maltego Carbon™, a penetration testing tool (often used by those working in cybersecurity), enables the capturing and exploitation of particular types of information from online spaces. Maltego Carbon 3.5.3 is the latest version of a tool which has been through various iterations since its inception in 2006 (Evolution -> Radium -> Tungsten -> Carbon). In its life span, this software tool has grown in sophistication. It may...
capture a broad range of information from the Surface Web to transform into open-source intelligence (OSINT). This software is created by Paterva, a South Africa-based software company. While the tool was designed for an adversarial context, it has wide potential application in academia and higher education.

In higher education as in other sectors, it is critical to deal with verifiable facts and to engage the world as it is. Competitive advantage lies in access to valid information for innovation, research, teaching-and-learning, administration, public relations, marketing, strategic messaging, fund-raising, and a wide range of higher education endeavors. Exploiting what is actually knowable with the given publicly-available software tools of an age (and minimal effort) is de rigueur and a critical aspect of transparency.

In a recent online book, Conducting Surface Web-Based Research with Maltego Carbon, the author summarized some of the software tool’s capabilities:

- “The mapping of the underlying technologies used for the hosting of a site;
- The linking of a disambiguated person to related email addresses;
- The geolocating of a Twitter account;
- The geolocating of various types of online information to physical spaces;
- The mapping of a Uniform Resource Locator (URL) to its related network and domain information;
- The identification of devices used on a particular Web network;
- The identification of a Net infrastructure for a website;
- The mapping of the cyber entities based on a certain physical location;
- The linking of a semi-disambiguated alias with personally identifiable information (PII);
- The link between an email address and a disambiguated individual;
- The link between a phone number to a disambiguated individual or other online information;
- The link between a disambiguated phrase with other online information;
- The mapping of social networks based on a Facebook account; and
- the mapping of social networks based on a Twitter account” (Hai-Jew, 2014).

This chapter builds on Conducting Surface Web-Based Research with Maltego Carbon by applying Maltego Carbon’s capabilities to six generic use cases in a higher education context. The use cases are conceptualized as examples. The topics to seed the cases were drawn from both the higher education context and the trending issues of the one day when the data extractions were conducted. The purpose of the data extractions were to showcase the tool and not to provide deeper insights about the particular topics. The six use case topics follow:

Use Case 1: Understanding an Online/Offline Entity.
Use Case 2: Exploring a Domain.
Use Case 3: From Physical Location to Cyber and Back Again.
Use Case 4: Online Conversations on Social Media Sites.
Use Case 5: Eventgraphing: Mapping an Event Online.
Use Case 6: Finding Leads to Enhance Research.

These are not comprehensive use cases, and these do not reflect the full capabilities of the tool. Within each case, there are numerous ways to conduct the data extractions. What is presented are some