Network Analysis and Visualization for Crime Prevention (NAVCAP)

User manual for network analysis software

By Andrew V. Papachristos
and Chris M. Smith

Recommended citation:
Papachristos, Andrew V and Smith, Chris M 2017. *Network Analysis and Visualization for Crime Prevention (NAVCAP): User Manual for Network Analysis Software*. New York, NY: National Network for Safe Communities.

Published 2017

Contents

About this User Manual

The Group Violence Intervention (GVI), a strategy of the National Network for Safe Communities (NNSC), attempts to reduce violence in a city by focusing a coalition of law enforcement, community, and social services at the small number of people driving a disproportionate amount of violence. This population is often involved in groups, otherwise known as gangs, sets, crews, cliques, or posses. Since the first group violence intervention in Boston, as Operation Ceasefire, effective implementation has depended upon accurately identifying the individuals involved in these groups, the dynamic within groups, and the relationships between groups. By debriefing front line law enforcement and violence prevention personnel, the Boston team used a marker and a large sheet of paper to diagram and make sense of the alliances and feuds between groups. Twenty years later, the motivation remains the same, but technological capability and data management systems have greatly improved. Moreover, subsequent empirical research has demonstrated that violence is deeply concentrated within and spread among social networks. This fact makes the analysis of social networks vitally important to violence reduction practitioners—to identify and address feuds between groups, as well as likely individual perpetration and victimization.

Powerful multipurpose software programs (such as R) and expensive proprietary network software have met the demands from police departments and violence prevention experts with technical expertise or significant resources. Other departments and agencies have contracted with outside agencies to conduct social network analyses at the outset of a crime reduction strategy, but they did not have the capacity to continue pursuing further analysis as needed during implementation. But now the Network Analysis and Visualization for Crime Prevention (NAVCAP) software is the first free network analysis software designed for widespread use by experienced analysts, as well as lay department personnel. NAVCAP offers practitioners the ability to map and analyze individual co-offending networks and group relationship networks without the need for coding or command line experience. This manual describes the installation, capabilities, and use of NAVCAP, using four educational modules. The software file, example data, and other resources are hosted at https://nnscommunities.org/our-work/innovation/social-network-analysis.

About Andrew V. Papachristos and Chris M. Smith

Andrew V. Papachristos is a professor of sociology and faculty fellow at the Institute of Police Research at Northwestern University. He is also a senior research advisor for the National Network for Safe Communities and a frequent collaborator and subject matter expert on network analysis for the Group Violence Intervention (GVI). His research focuses on social networks, neighborhoods, street gangs, and interpersonal violence.

Chris M. Smith is an assistant professor of Sociology at the University of California, Davis. Her research focuses on criminal networks, crime and inequality, and police violence.

About the National Network for Safe Communities

The National Network for Safe Communities (NNSC) was launched in 2009 under the direction of David M. Kennedy. NNSC focuses on supporting cities implementing proven strategic interventions to reduce violence and improve public safety, minimize arrest and incarceration, strengthen communities, and improve relationships between law enforcement and the communities it serves. The Group Violence Intervention, first developed in Boston as Operation Ceasefire, has effectively reduced violence in cities as diverse as Chicago, Illinois; Cincinnati, Ohio; New Orleans, Louisiana; and Stockton, California. NNSC has also applied the principles of its strategic intervention to eliminate drug markets in many U.S. cities through the Drug Market Intervention, reduce juvenile violence and robbery, and address domestic violence. Substantial research and field experience have proven that these interventions are associated with large reductions in community violence and disorder.

NNSC believes that these successes mean that cities can deal effectively with their crime problems in a fundamentally different way—reducing violence while simultaneously transforming toxic law enforcement and community relationships to help communities step forward and reset their own antiviolence standards. NNSC provides technical advising to jurisdictions around the country that are currently implementing interventions and facilitates collaborative working sessions to facilitate distance learning; address common issues; provide a supportive community of practice for new jurisdictions; and make these interventions standard practice across the United States.

Introduction

Social network analysis (SNA) in the field of criminal justice is no longer limited to oversized corkboards covered in photographs of suspects and tacked red strings mapping their connections. This classic investigatory organizational tool has moved to computers with new software applications. However, the original logic still applies—people are connected to other people—and figuring out the connections between people helps us understand why people do the things they do.

Social networks are the large systems of social connections and social relationships in which individuals are embedded (Christakis and Fowler 2009; Kadushin 2012). Social relationships can include friendships, work relationships, neighbor relationships, associations with classmates, gang affiliations, or any of the other various ways in which we are connected with others. Most importantly, the people with whom we are connected and the ways we are connected to them affect what we feel, think, and do.

Social network concepts are prevalent in day-to-day life. Familiar phrases referring to social networks include "It's not what you know, but who you know," which points to the notion that skills and talents are often secondary to the social connections one has with others in the business or work world. "It's a small world" refers to those moments when individuals realize their overlapping connections to others—a friend of a friend is a friend. A synonym for the "small world" phenomenon is "six degrees of separation," which references the theory that everyone can be connected to everyone else in six handshakes or less (Travers and Milgram 1969; Watts 2003). The "old boys' network" can refer to actual groups of male pupils or a metaphor for cronyism, and this idiom implies that personal social ties are the key to individual success. Central to all of these day-to-day phrases is the idea that social networks are a meaningful and influential part of the social world.

There is an entire science dedicated to the study of social networks. Social network analysis measures and maps out the social connections and relationships between individuals (Christakis and Fowler 2009; Kadushin 2012). This information on relationships is combined with powerful analytical tools in order to empirically test the various ways in which social networks form, grow, or influence behavior.

What is a Social Network?

A classic definition of social networks comes from Stanley Wasserman and Katherine Faust's 1994 book, titled *Social Network Analysis: Methods and Applications*. Wasserman and Faust define social networks as "a finite set or sets of actors and the relation or relations defined on them" (Wasserman and Faust 1994:20). Their definition proposes two essential features of social networks: the actors and their relations. We could choose to study just actors and their actions or beliefs—much research does this. However, when we only study actors, we ignore the larger social networks that surround those individuals, and we forget that individual actions and beliefs are influenced by systems of relationships. We do not want to forget this larger system of influence when we think about individuals; however, a social network requires both the actors *and* their relationships.

Social networks allow for powerful and meaningful visualizations. Our eyes are incredibly efficient at identifying patterns and connectedness between individuals when their relationships are presented in a social network format. For example, Figure 1 below could represent five individuals. From this visualization of a social network we can see that all five individuals are connected to each other. A network such as this might represent a close set of friends or a small working group. The mapping of their relationships provides us with more information than analyzing these individuals in isolation.

Social Network Applications

Social network analysis has been used to research a range of topics: the spread of disease (Morris and Kretzschmar 1997), political influence (Mcclurg 2003), opinions (Watts and Dodds 2007), behaviors (Christakis and Fowler 2009), friendships (Wimmer and Lewis 2010), marriages (Bott 1957), human societies (Apicella et al. 2012), and animal societies (Croft, James, and Krause 2008). In criminology and criminal justice, social network analysis has been used to study the diffusion of homicide in high-risk networks (Green, Horel, and Papachristos 2017; Papachristos and Wildeman 2014) as well as social status and support among prisoners (Schaefer et al. forthcoming). Various scholars have studied the structure of criminal groups, including terrorist organizations (Krebs 2002; Pedahzur and Perliger 2006), motorcycle gangs (Morselli 2009), street gangs (McGloin 2005; Papachristos 2009), drug trafficking (Bright, Hughes, and Chalmers 2012; Malm and Bichler 2011), and organized crime (DellaPosta forthcoming; Mastrobuoni and Patacchini 2012; Smith and Papachristos 2016).

Figure 1. Example of a Social Network

Social network analysis answers questions common to criminal justice and criminology through different approaches to networks. One criminal justice application is to use social networks to study the structure of criminal groups or criminal networks; for instance, mapping out the network of an entire criminal group could tell us how cohesive a criminal group is. We could learn if the group's structure is hierarchical or flat, dense or sparse, connected or disconnected. Or, we could use the social network analysis to identify the important, central, or powerful players in the criminal group.

A second approach to social network analysis in criminal justice applications is to map out broader social relationships to identify the contexts in which crime and deviance occur. For example, social network analysis has been used to look at the influence of peer networks on criminal activities and delinquent behaviors among adolescents, such as peer influence on smoking and petty theft (Haynie 2001). Crime and delinquency occur in a larger context of social networks. Similarly, shootings or other violent events
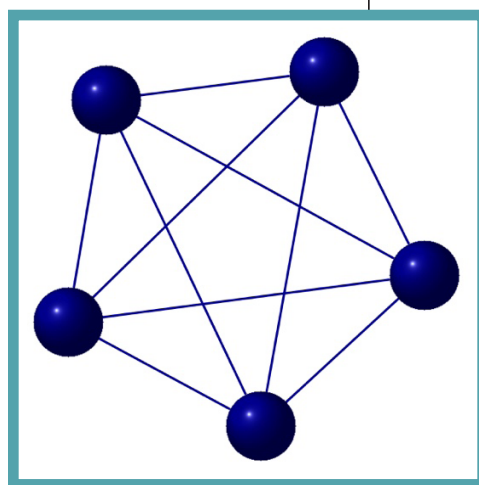
can be identified in larger contexts such as arrest networks or affiliation networks (Green, Horel, and Papachristos 2017; Papachristos and Wildeman 2014). Mapping out the rivalries and alliances between criminal groups, such as gangs, can help pinpoint where violent exchanges might be more likely to occur (Sierra-Arevalo and Papachristos 2015).

A third approach considers relationships as a conduit for transferring material items or information. The social network analysis could map out: the path of exchanges of drugs, money, or guns; violent events, training, or the spread of information; or the path of a single weapon exchanged over time among associates.

Analyzing Social Networks

Analyzing social networks requires two pieces of information. The first piece of information consists of the actors in a network; visually, these actors are represented as nodes or the dots (also sometimes called vertices). In the figure below are three nodes labeled with the letters a, b, and c.

The second piece of information required is the edges or the lines between the nodes, which represent relationships or ties. There are three edges in the example below: the edge between nodes a and b (a, b), the edge between nodes b and c (b, c), and the edge between nodes a and c (a, c). As indicated in the definition above, both pieces of information are essential to social network analysis.

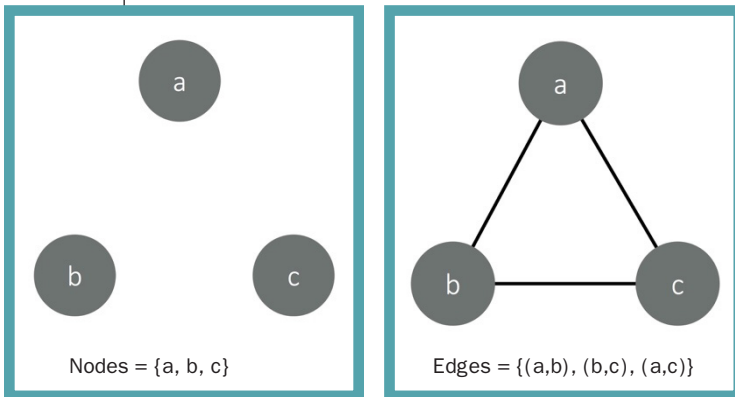Nodes = {a, b, c}   Edges = {(a,b), (b,c), (a,c)}

Figure 2. Nodes and Edges of Social Networks

In this small example network, all three nodes have ties to each other. This is a simple network of three nodes, but the same logic extends to networks of all sizes. Imagine cases in which multiple people were arrested together. Each node could be a person, and each edge could indicate the co-arrest. Criminal justice arrest data are often detailed enough to produce meaningful networks. For example, Figure 3 shows a co-arrest network from New Haven, Connecticut, over a three-year period. This network contains 513 people and more than 803 incidents of co-arrest between them—in this case, a person is linked to another person *through* a co-arrest (e.g., two people would have a tie when they are arrested for committing a crime together). Similar to co-arrest networks found in published research in Chicago, Boston, and elsewhere, Figure 3 shows that co-arrest ties can link individuals into a much larger network (perhaps invisible to even those who are included in it) that might affect people's behaviors, opinions, or attitudes. For example,

the structure of this network might affect people's risk of gunshot injury (Papachristos and Wildeman 2014). Identifying such co-arrest networks might also serve as a platform for the interventions described above by providing information on individuals or parts of the network that might be more susceptible to intervention or prevention efforts.

NAVCAP Goals & Objectives

Social network analysis (SNA) will not solve the gun violence problem in the United States, nor will it somehow magically fix police and community relationships. However, social network analysis can help violence prevention efforts by using data to inform our interventions—thus focusing on rather than widening the points of contact police have with the community. More than that, efforts by the NNSC—such as the Group Violence Intervention (GVI) initiative—coordinate collaborations that are transparent in process and directed in efforts. These collaborations have united police and communities around violence prevention efforts for more than two decades. Network analysis is just one data-informed approach that has the potential to support violence prevention efforts.
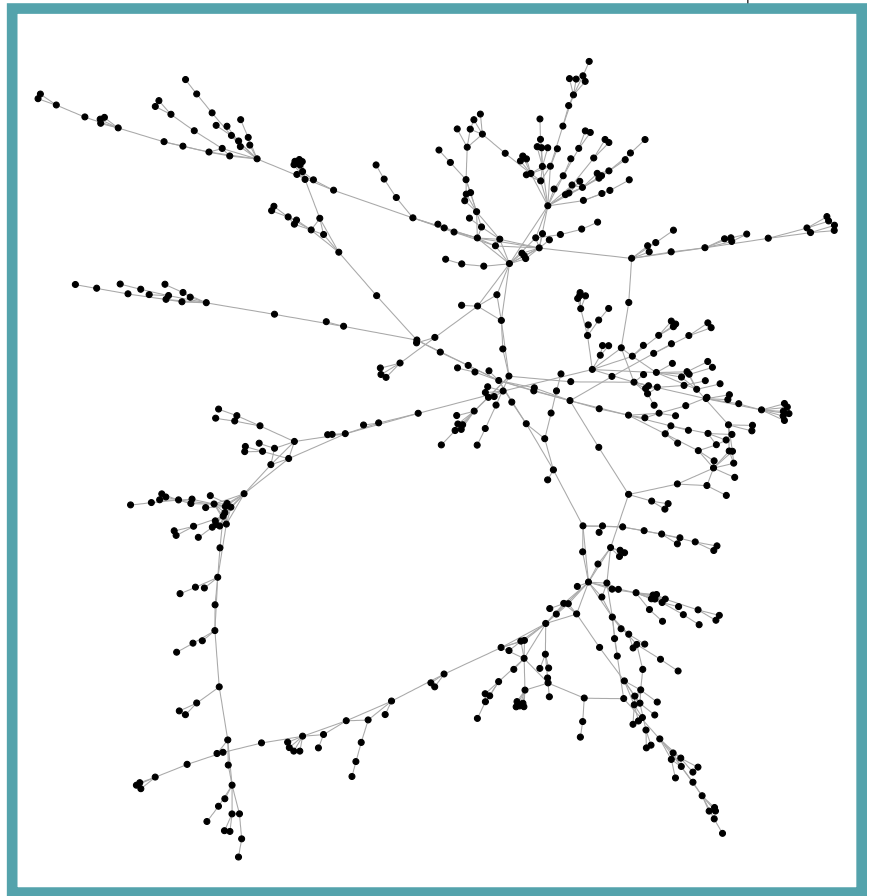

Figure 3. Example of a Co-arrest Network in New Haven

This leads us to Network Analysis and Visualization for Crime Prevention or NAVCAP, the piece of software described in this manual. The NNSC and its associates have been integrating social network analysis into the GVI since the 1990s. Over the last decade, NNSC has worked with various academic partners to provide analytic support for

partner cities and departments. The expansion of GVI and related efforts—as well as the diffusion of affordable computers and software—have increased the demand for such data analytics and support. While an array of network software solutions exists, many are extremely expensive and beyond the reach of city or departmental budgets. At the same time, the technical know-how for conducting network analysis also presents a somewhat steep learning curve for practitioners.

NAVCAP and its training materials provide an easy-to-use introduction to social network analysis for organizations, schools, departments, and programs interested in applying SNA to crime and violence prevention efforts. These pages will provide a step-by-step guide for software designed to visualize and conduct basic analyses on networks of groups and individuals who are often involved in gun violence. There are no predictive models in NAVCAP; in other words, nothing that will tell you what to do, or when to do it. That is not the point. Computers and data analytics should never replace human intelligence or the expertise of those working in our communities. Rather, NAVCAP will help map particular social problems and provide a tool to reorganize available data and expertise. These maps must be read (and re-read) by those using them to inform strategic decisions, but the networks cannot make decisions on their own. NAVCAP is being used by NNSC partners across the country in their GVI and other efforts. By providing you with this manual, we hope to provide one more useful tool in the effort to curb gun and group violence.

This manual is organized into four modules: (1) Introduction, (2) Data, (3) Visualization, and (4) Analytics. 'Module 1: Introduction' presents the NAVCAP software and assists participants with installing it on their personal or work computers. 'Module 2: Data' explains the data formats required for NAVCAP. In Module 2, participants will format a spreadsheet to be compatible with NAVCAP; load spreadsheets into the software; and learn the different accompanying files loadable in NAVCAP. 'Module 3: Visualization' introduces participants to various plotting options in NAVCAP and demonstrates how to customize network images. 'Module 4: Analytics' explains the filter options and neighborhood tools to analyze co-offending networks.

MODULE 1: INTRODUCTION TO NAVCAP

Goal:

NAVCAP is Network Analysis and Visualization for Crime Prevention. Participants will install NAVCAP for social network analysis on their personal computers in preparation for the NAVCAP track in the remainder of the modules.

Computer Requirements

The prerequisites to install the NAVCAP software are as follows:

- Admin privileges for the computer on which you want to install the software
- Windows 7 or higher with a C Drive
- Microsoft .NET Framework 4 or above
- 4GB RAM or more
- 32 bit OS or above

If your computer meets these requirements, then you are ready to proceed with the download and installation of the NAVCAP software.

## Installing NAVCAP Software for Social Network Analysis

Computer programmers designed NAVCAP software specifically to meet the social network and institutional data needs of criminal justice practitioners and analysts. NAVCAP runs a few programs in the background on your computer, and all of these required background programs are included with the NAVCAP installation.

Note: Some of the screenshots in this document predate the naming of the NAVCAP software and might not exactly match those on your screen.

1. Download the NAVCAP Installer folder from the website hosting all of the materials for the SNA for CJ training.
2. If the folder is zipped, right click on the folder and select "Extract All" in order to unzip the folder. Put the unzipped folder in a place on your computer where you can easily access it.
3. Double-click the NAVCAP_Installer icon.

SNACN_Installer

4. Depending on your computer's security levels, you might receive a pop-up about whether you want to trust this download from the internet. As long as you followed the link provided, this is safe software to download to your computer.

5. The NAVCAP_Installer Set-up Wizard will open. Click the `Next>` button located in the lower right corner of the window.
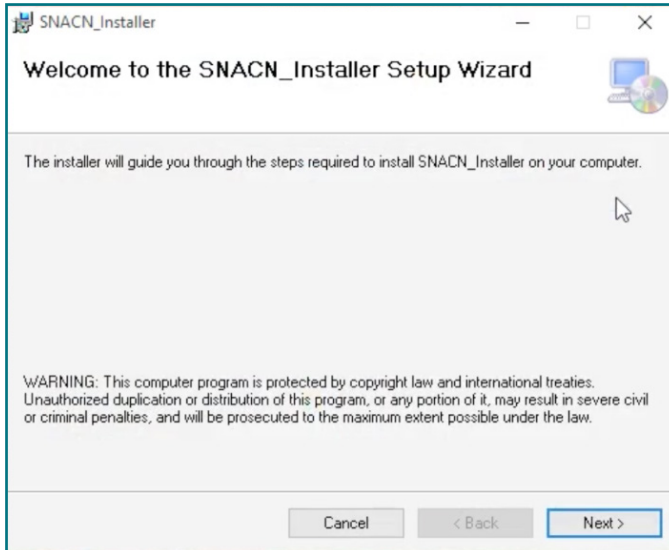

6. This brings you to the Select Installation Folder screen. We recommend that you use the default settings that automatically populate in the folder path. You should decide if you want to install NAVCAP for all users of the computer or just your user account, and select the appropriate radial button. Then click the `Next>` button.
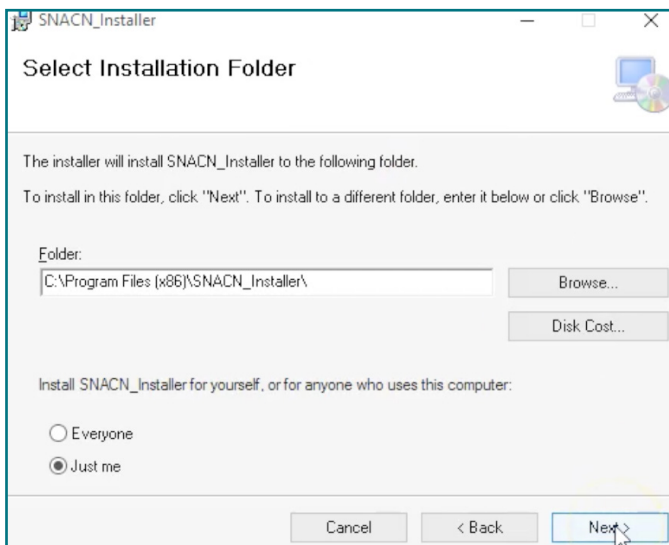
7. This brings you to a screen to Confirm Installation. Click the `Next>` button to confirm installation.
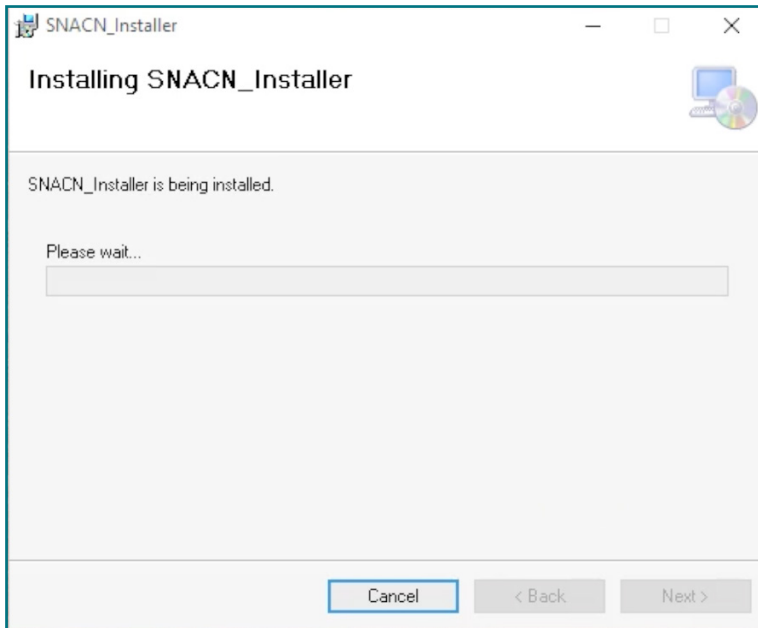
8. This will begin the NAVCAP installation. Depending on your computer's security settings, you might have to confirm that you want to continue with the installation.

9. Once the installation is completed, a new icon with the name `NAVCAP.exe` will appear on your desktop.
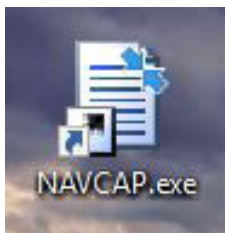
10. Click on the NAVCAP.exe icon to open the window for the NAVCAP Prerequisite Check. Some of the required background programs will likely need to be installed if this is your first time opening NAVCAP. To install the remaining necessary applications, check the boxes for the programs that are `Not Installed` from the list, and then click on the blue `Install Required Software` button at the bottom of the window.
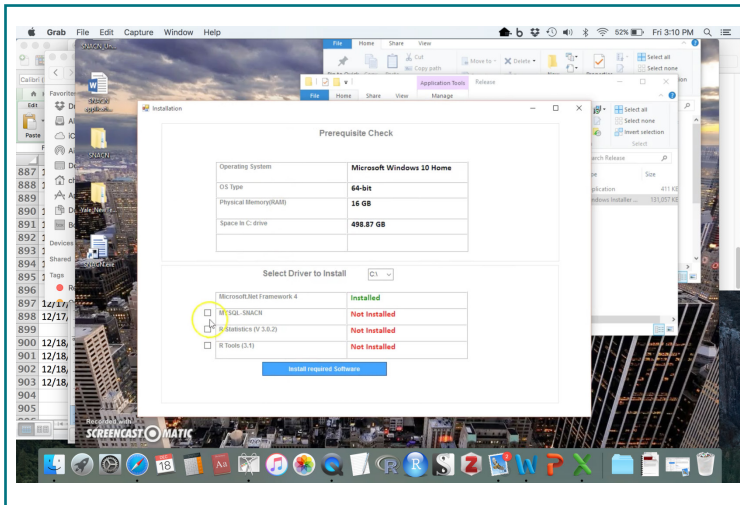
11. Wait while the various programs are being installed. Once they are all correctly installed, each program on the list will change from a red `Not Installed` to a green `Installed`. Click on the blue `Continue to Application` button to launch the application.

Network Analysis and Visualization for Crime Prevention (NAVCAP)
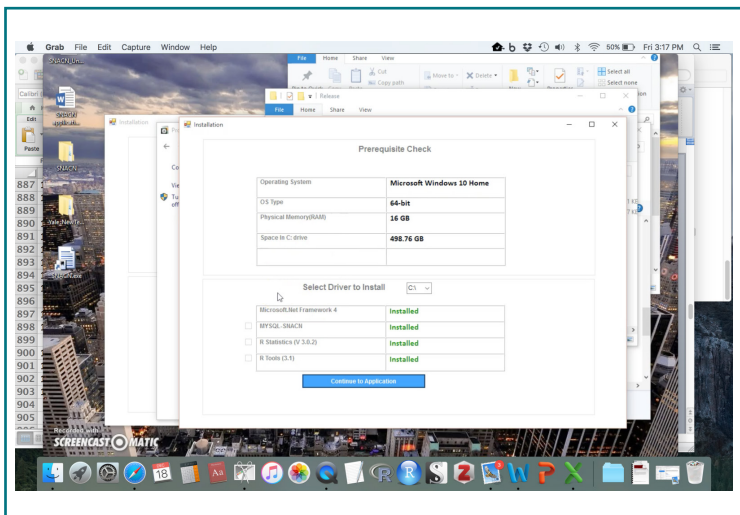
12. Welcome to NAVCAP. If everything installed correctly, you should see the NAVCAP program open and ready to upload your data. (Refer to Module 2: Data NAVCAP Lab for the next steps.)
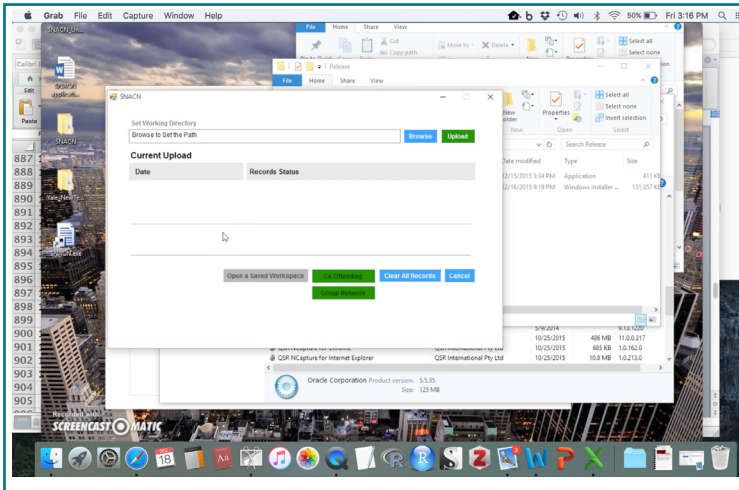
Troubleshooting Installation

The NAVCAP software requires particular versions of several free programs that will run background processes for NAVCAP. The NAVCAP installer works best on a computer that meets the computer requirements listed above and has never installed some of the background programs.

You may face a problem during installation if your computer already has MySQL installed. MySQL is a common open-source relational database management system that, when installed, will create a MySQL folder on the C drive of your computer. If you already have MySQL on your computer, the NAVCAP installer will not be able to install MySQL again for you. In this case, you can either uninstall MySQL (assuming that you do not use it for other software) or provide your MySQL credentials (username and password) when prompted in the pop-up screen.

The NAVCAP installation was designed not to overwrite newer versions of R and Rtools. If you have ever installed the R statistical program on your computer and have a newer version than the one used in the background of the NAVCAP software, you should not have to uninstall your newer version of R and Rtools. However, you might notice that an older version of R also appears on your computer, which is compatible with the NAVCAP program. If you have problems with the R portion of the installation, you can uninstall all versions of R and Rtools from your computer. Run the NAVCAP_installer again to get the version of R required for NAVCAP, and then you should be able to re-install the newest version of R. It is possible to have multiple versions of R downloaded on to the same computer.

The programs listed below might cause problems with the NAVCAP installer, and might require uninstalling in order to successfully install NAVCAP:

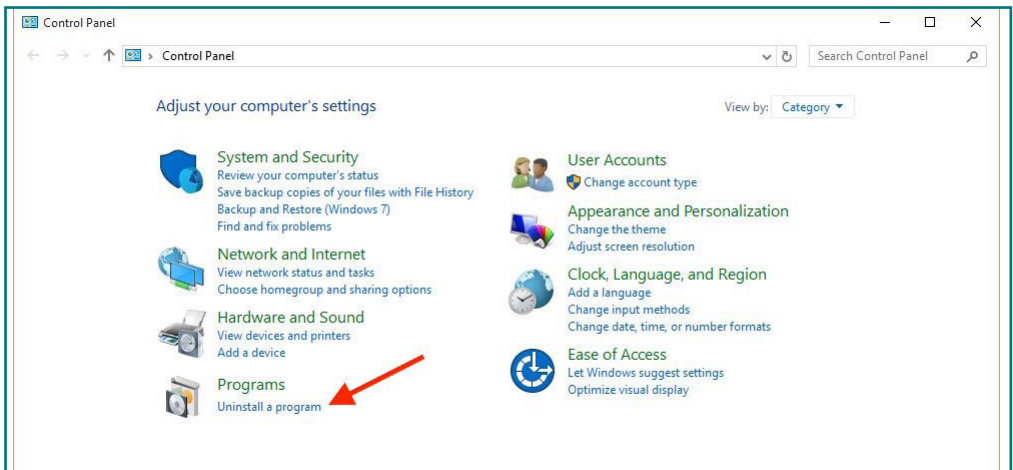NAVCAP_Installer (previous downloaded version)

MySQL Server

R for windows 3.0.2

Rtools 3.1

To properly uninstall software from a Windows computer:

1. Go to the application Control Panel
2. Click on the `Uninstall a program` link underneath Programs.

3. Locate any programs from the list above that might be installed on your computer that you want to uninstall.
4. Right click on the programs to uninstall, and follow any necessary prompts.
5. If you have MySQL on your computer and you want to remove it, you will also need to go to your C Drive folder and delete the MySQL folder from your C Drive.
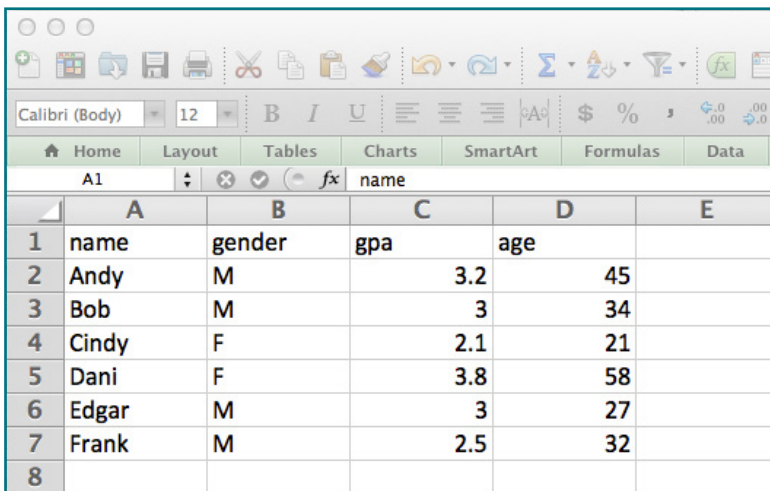
MODULE 2: DATA

Goals:

Participants will format a spreadsheet to be compatible with NAVCAP software. Participants will load spreadsheets into the NAVCAP software. Participants will become familiar with the different accompanying files loadable in NAVCAP software. Participants will differentiate between the arrest-level analysis and the group-level analysis.

CSV Files

CSV is a file extension that stands for "comma separated values." A CSV file is essentially a text file in which information is separated by commas. A CSV is a non-program specific file format that allows spreadsheet software to read text and organize it into rows and columns. Spreadsheet software, like Microsoft Excel, automatically organizes text into different cells of a table based on the location of the commas. CSV files are versatile files that can be read easily by many software programs than can read text or spreadsheets on any computer. Below is a screenshot of a sample CSV file. It is a spreadsheet that contains seven rows and four columns.
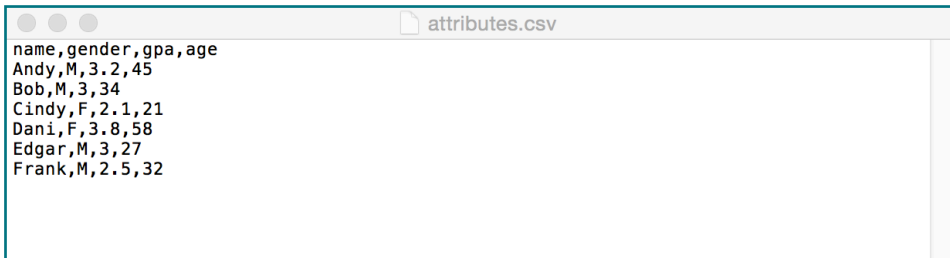

When you open a CSV file in a text-editing program (such as TextEdit on Macs or Notepad on Windows), you get the same information, but you can see the text separated by commas that underlie the CSV file. The same seven rows seen in the spreadsheet software are in the text-editing program, but instead of four columns, each

row contains three commas separating the data that would otherwise belong to each separate cell across four columns.

```
●  ●  ●                        📄 attributes.csv
name,gender,gpa,age
Andy,M,3.2,45
Bob,M,3,34
Cindy,F,2.1,21
Dani,F,3.8,58
Edgar,M,3,27
Frank,M,2.5,32
```

The CSV file format is compatible with NAVCAP, and easily imports data into the software. CSV files designed on Mac computers tend to not be recognized by NAVCAP software. If you build a CSV file on a Mac computer for NAVCAP, you will need to open the CSV file on a Windows computer and save and replace the file before attempting to upload the file to NAVCAP.

Arrest.csv

The main data file for the NAVCAP application is the `Arrest.csv` file. Even if the spreadsheet does not contain actual arrests, it needs to have this exact `Arrest.csv` file name for identification purposes within the software. NAVCAP can accommodate information on hundreds of thousands of individuals or events through this single file.

The `Arrest.csv` is a two-mode dataset connecting people through events and events through people. You can review the differences between one-mode and two-mode data in the tutorial portion of Module 2.

The `Arrest.csv` file must contain the three following pieces of information to load correctly in NAVCAP:

(1) Person ID: This is some alphanumeric code that uniquely identifies each person in the data. Each individual has exactly one such code that is associated solely with that individual and continues to be associated with that same individual across events.

Example:
Andy and Christin are arrested together for an attempted armed robbery. In a department's arrest records, Andy and Christin are each given unique individual identifiers called Person IDs. In this case, Andy's Person ID is T123 and Christin's is H456. The NAVCAP software requires each person to have a unique person ID, so the analyst takes the information from department records to begin a dataset for NAVCAP that starts like this:

```
Person ID              Case ID              Arrest Date
T123
H456
```

Important note: NAVCAP cannot handle apostrophes, as it will return an error when the data is loaded. Therefore, removing all apostrophes from names and Person IDs is required.

(2) Case ID: This is some alphanumeric code that uniquely identifies each event or case in the data. This is often an arrest number, a booking number, or incident number. The Case ID has to be the same for all people associated with the same event, but the Case IDs should not be reused across different events.

Example:
Because Andy and Christin were arrested together for committing the robbery together, they need to share a case identification number. In this example, the Case ID for their robbery is GP5305. From this simple two-mode event data format, NAVCAP will link the unique individuals (Andy and Christin) through the Case ID forming a network tie.

```
Person ID              Case ID              Arrest Date
T123              GP5305
H456              GP5305
```

(3) Arrest Date: This is typically a date associated with each event. If you do not have the actual event date, you can enter in any date such as the date you typed the data. This will not affect the analysis. The date of the event is used to filter data and is required to properly load the `Arrest.csv` in the NAVCAP program.

Example:
Andy and Christin committed their robbery on August 23, 2002. We add the date of their event to the Arrest Date column. If we didn't know the date of the event, we would just enter some real past or present date in this column. This ensures that the database will load properly. Avoid using future dates if you do not know the exact date of the event.

```
Person ID              Case ID              Arrest Date
T123              GP5305              08/23/2002
H456              GP5305              08/23/2002
```

Now that we are familiar with the three column requirements of the `Arrest.csv` file for NAVCAP, let's work on mastering the formatting requirements for the `Arrest.csv` spreadsheet. The good news is that most arrest records are similar enough to the NAVCAP requirements that reformatting official arrest records should just take just a little bit of work in your spreadsheet software. The bad news is that small mistakes in the spreadsheet might cause the data not to load, and small mistakes can be difficult to diagnose. Let's start by constructing our very own fake `Arrest.csv` in Microsoft Excel of a small network before working with a larger example. Follow the instructions below to craft an `Arrest.csv` of your own.

1. Open a new spreadsheet file in Excel or your computer's spreadsheet software.

   Located in your `Data NAVCAP Files` folder for Module 2 are three subfolders: `Cooffending`, `Group`, and `Yours`. See the screenshot below. Locate this set of subfolders on your computer.
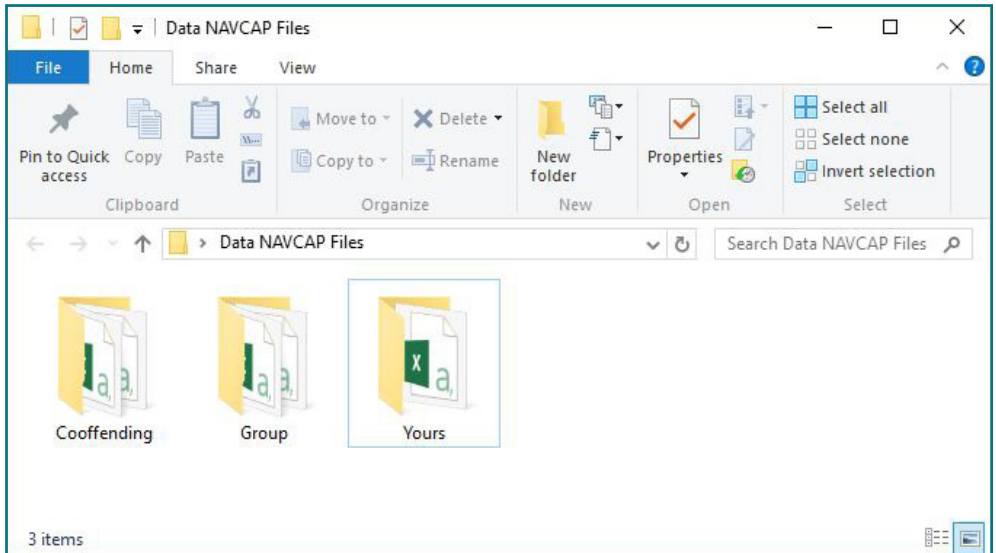

   One tricky aspect of NAVCAP is that once you specify a working directory for your session, NAVCAP will then look for the files with the correct and exact file names. A single folder on a computer cannot contain multiple files with the same names—you cannot have two files both named `Arrest.csv` located in the same folder. However, you might have multiple datasets that you want to analyze within NAVCAP. Subfolders are an easy and necessary solution to this tricky issue. The three subfolders contained within the `Data NAVCAP Files` folder for Module 2 will keep different files with the name `Arrest.csv` separate. Save your new practice spreadsheet to the `Yours` subfolder. This will avoid overwriting the sample data provided for this lab in the `Cooffending` subfolder and still allow you to name your example `Arrest.csv`.

2. Save your newly opened and currently empty spreadsheet in the `Yours` subfolder with the exact file name: `Arrest.csv`

   The default format to save files in Microsoft Excel is an Excel workbook with the extension `.xlsx`. We need to override this `.xlsx` default by selecting `Comma Separated Values (.csv)` next to `Format` under the save option. This will change the file extension. You should not need to type the `.csv` in the file name of `Arrest.csv` because changing the file format automatically changes the file extension.

You should be able to see the complete file name at the top of your Excel window. If not, return the `Yours` subfolder to inspect the file name and file format. Once you are satisfied that the file is saved correctly, you can begin filling in the spreadsheet. First we will add the header row.

3. In row 1 of the `Arrest.csv,` type the following headings exactly as they appear below. Replicate the order. Be sure to include only a single space between words and no spaces after the last word of each cell. Replicating the capitalization is not necessary, but it is recommended. There are 11 headings, so you will use columns A through K in the spreadsheet, typing one heading per cell in the following order across the first row.

```
Person ID
Case ID
Arrest Date
Event Type
Address
District
DOB
Name
Offense Description
Gender
Race
```

Hopefully some of these headings look familiar to you, and you can imagine the equivalent headings that your agency uses. At this stage, your results should look like this screenshot below.

Now we can add some examples. Let's create two group arrest events. The first arrest will contain 3 people and the second arrest will contain 4 different people.

4. Create 3 unique Person IDs to represent the 3 people in the first group arrest. Person IDs can be names, numbers, or a combination of letters and numbers. They just need to be unique to each person. Create a unique Case ID number for this group arrest. Case IDs can also include letters and/or numbers. The Case ID will be the same for the 3 people in this group arrest. Create an Arrest Date for this event. We recommend choosing a date that has passed in the last year. (This is because we will use the calendar function as a filter to check that our data loaded correctly, and more recent dates will help you avoid scrolling through months of calendars to find your dates.) Avoid using future dates. Optionally, you can fill in some of the other columns of this spreadsheet.

5. Repeat the previous step for a second group arrest that includes 4 people. You will need 4 new Person IDs and 1 new Case ID. The date can be the same or different

Here is an example screenshot of this exercise that will upload correctly in the NAVCAP software.

Network Analysis and Visualization for Crime Prevention (NAVCAP)
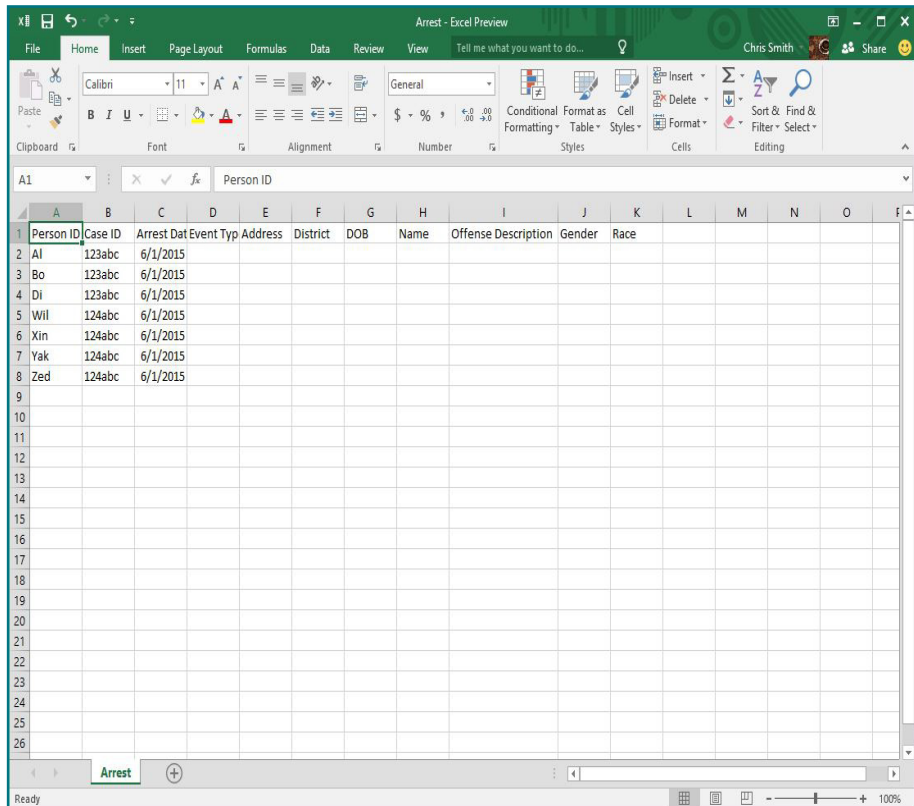
6. Save your `Arrest.csv` and close Microsoft Excel.

    This lab includes another prepared `Arrest.csv` file that you can practice loading into NAVCAP software. This file is stored in the `Cooffending` subfolder located in the `Data NAVCAP Files` folder in order to avoid conflict between files with the same name. Open this premade `Arrest.csv` now to examine its contents. Be sure that the `Arrest.csv` from the previous task is closed. What differences do you notice between it and the one you made in the previous task?

	A	B	C	D	E	F	G	H	I	J	K
1	Person ID	Case ID	Arrest Date	Event Type	Address	District	DOB	Name	Offense Description	Gender	Race
2	62914	302997	1/1/15							M	BLK
3	78636	313035	1/1/15							M	WHI
4	173642	313035	1/1/15							M	BLK
5	158190	313815	1/1/15							M	BLK
6	14056	314346	1/1/15							F	BLK
7	17700	320670	1/1/15							M	BLK
8	141447	326823	1/1/15							M	BLK
9	206115	326823	1/1/15							M	BLK
10	29311	329022	1/1/15							M	BLK
11	26524	329952	1/1/15							M	BLK
12	22522	336129	1/1/15							M	BLK
13	59191	337167	1/1/15							M	BLK
14	31596	338463	1/1/15							F	BLK
15	118104	338463	1/1/15							M	BLK
16	40358	340950	1/1/15							M	BLK
17	61981	343770	1/1/15							M	BLK
18	78636	344529	1/1/15							M	WHI
19	173642	344529	1/1/15							M	BLK
20	210095	345018	1/1/15							M	BLK
21	81859	345768	1/1/15							M	BLK
22	7553	346989	1/1/15							M	BLK
23	163316	346989	1/1/15							F	BLK
24	159757	347646	1/1/15							F	WWH
25	42606	349839	1/1/15							M	BLK
26	6956	351876	1/1/15							M	BLK

Close all of the CSV files that you may have inspected up to this point in preparation for loading the files into the NAVCAP application.

Loading Arrest.csv into NAVCAP
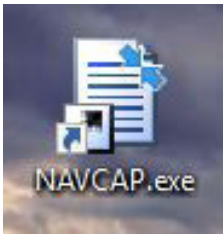
Likely there will be an icon on your desktop from the NAVCAP installation process completed in Module 1. If you do not see a desktop icon similar to the icon above, then search and locate NAVCAP among other programs on your computer.

Note: Some of the screenshots for this lab were taken from an earlier version of the NAVCAP application and might not exactly match the images on your screen.

1. Open the NAVCAP application on your computer.

   This will bring you to the Prerequisite Check window. Hopefully, everything installed correctly during Module 1 as indicated by the list of green `Installed` confirmations.
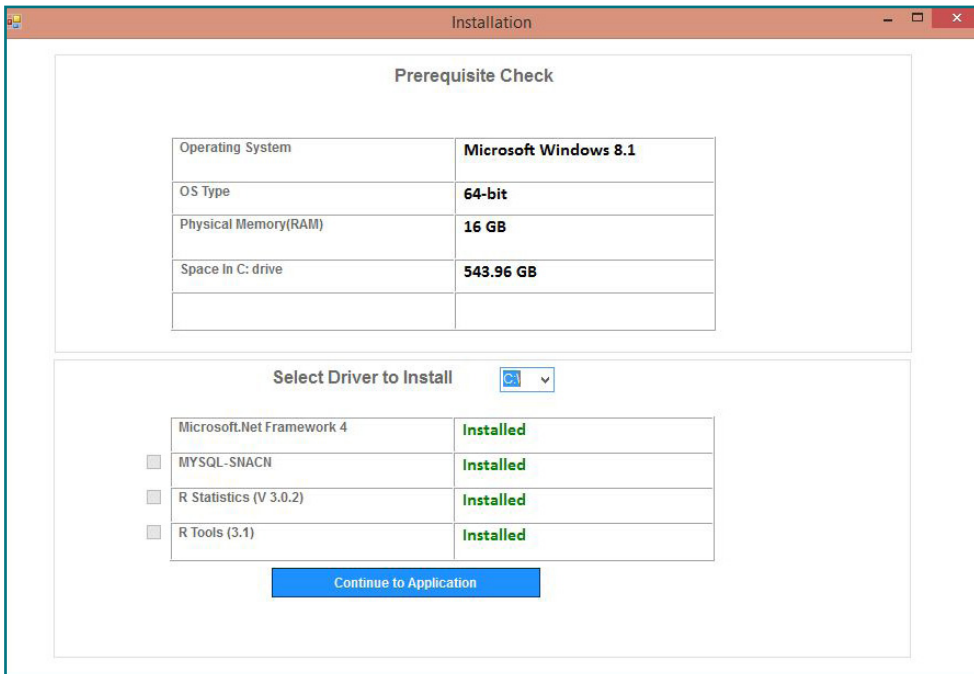
2. Click on the blue `Continue to Application` button at the bottom of the window.

   This brings us to the first window of the NAVCAP application where we upload our data. If you uploaded any data in a previous NAVCAP session, then you might see the counts stored here under Records Status.
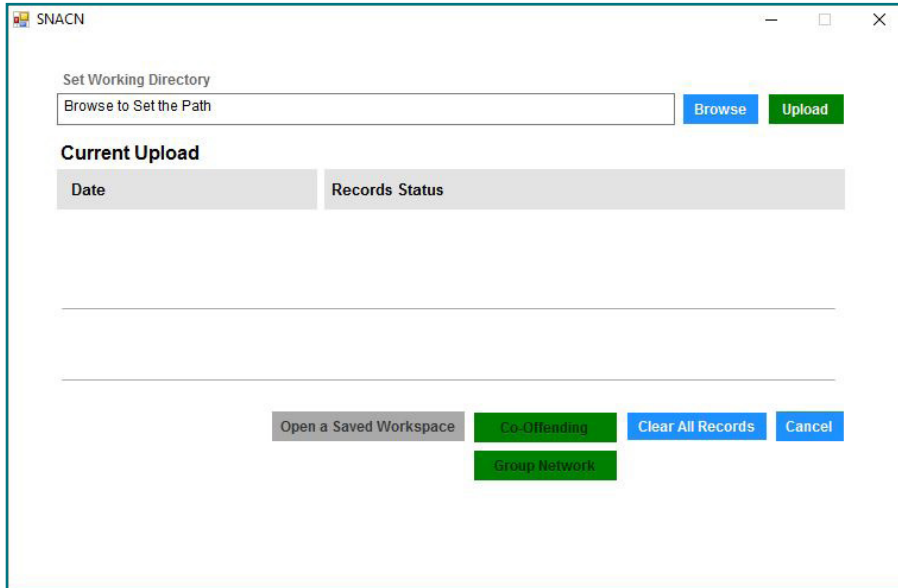
   First, let's upload the practice `Arrest.csv` that you made of the two group arrests. We stored this file in the `Yours` subfolder within the `Data NAVCAP Files` folder for the module.

3. Click on the blue `Browse` button toward the top of the window. Locate the `Yours` subfolder. Click `OK`.

   You will see your computer's path to the `Yours` subfolder now located in the `Set Working Directory` bar.

4. Click on the green `Upload` button next to `Browse` to see if the software can find the `Arrest.csv` file that it needs.
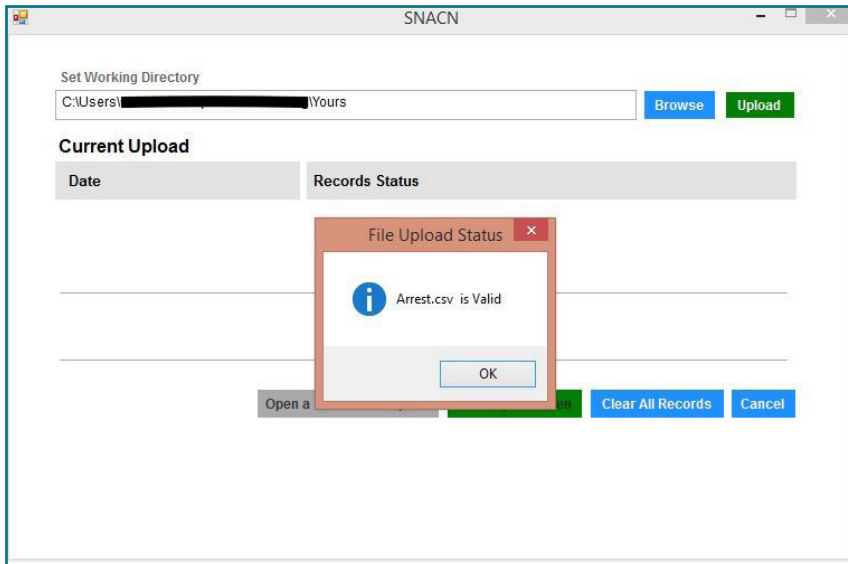
You should see the `File Upload Status` pop-up window. This means that the NAVCAP software recognizes your `Arrest.csv` file.

5. Click the `OK` button in the pop-up validation window to begin the upload of your `Arrest.csv` file, and watch your data load.

Network Analysis and Visualization for Crime Prevention (NAVCAP)
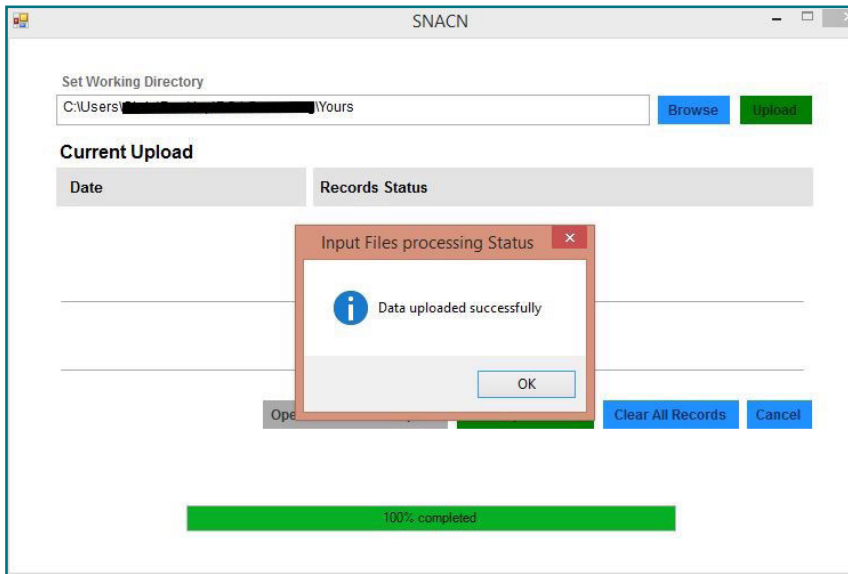
6. The `Input Files Status` box will show if the data uploaded successfully. If the data uploaded successfully, then click the `OK` button in the pop-up window to see how many records imported.
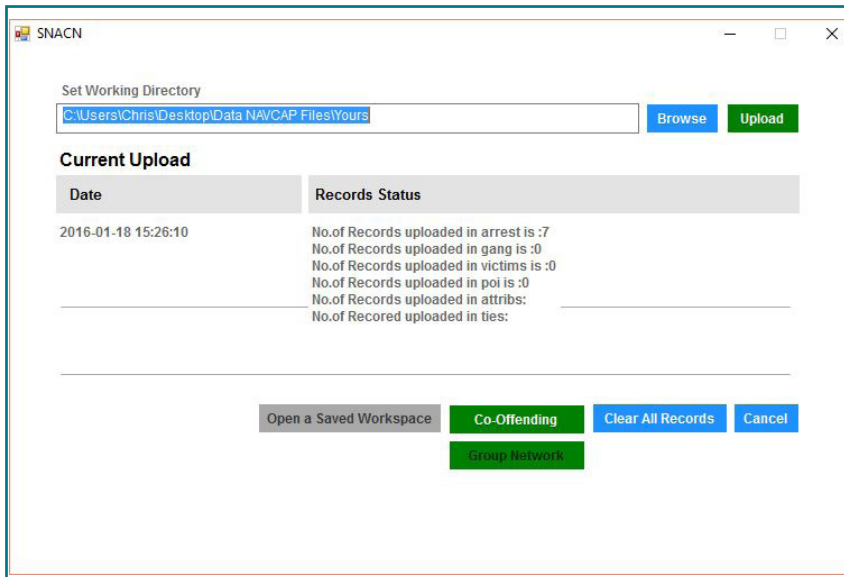
As you can see in the top row of Records Status, we have 7 records of arrests in the practice `Arrest.csv` file. You can also see the time that you uploaded these data, which might be useful if you return to the NAVCAP software at a later time.

Let's make a basic network image now to check that we structured the `Arrest.csv` file correctly. Recall that we tried to create an `Arrest.csv` file that would display 1 group arrest of 3 people and 1 group arrest of 4 people. Using the most basic graphing commands, we can inspect the practice `Arrest.csv` file.

7. From the Upload window, click on the green `Co-Offending` button located near the bottom of the window, which will take you to a new Seed List Filters window shown in the screenshot below.

This screen is designed to extract small sections of your network of interest based on particular filters. For present purposes, our network is so small that we just want to make a network image of the entire dataset. In order to do this, we use the Connections and the Arrest Date Range filters.

8. Scroll through the calendars in the Arrest Date Range to select the earliest date you entered in your `Arrest.csv` and the latest date you entered in your `Arrest.csv`. Earlier, we recommended using past dates of this year, so hopefully you do not have to click through too many calendar months to get to the beginning of your time period. The end of your date range can be today's date, since that range should cover what we put in our example `Arrest.csv`. You can also leave the Arrest Date Range empty—by not selecting dates, NAVCAP runs the entire dataset and avoids the date-filter issue.

9. Click on the dropdown arrow underneath Connections and select the number 1. We will go into more detail about values higher than 1 in Module 4: Analytics, but for now we are telling NAVCAP to include the direct connections to every person arrested within our date range or every person within a single tie of those arrested within our date range. This will include everyone in the network because of the date range.
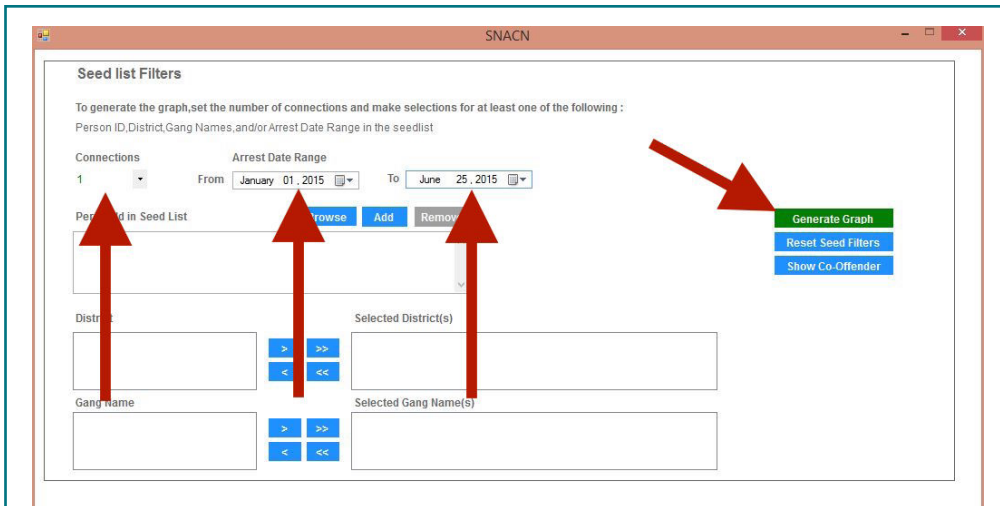
Once the Connections and the Arrest Date Range filters are set, we can generate the network.

10. Click on the green `Generate Graph` button located on the right side of the window.

Voila! A new window will open, containing the arrest network using the default plotting settings of NAVCAP. If everything went accordingly, you should have a triangle for a group of 3 and a square with an X through it connecting a group of 4. More on customizing network images in Module 3: Visualization. Your network might have a slightly different layout than the example below, but the nodes and edges should be similar.
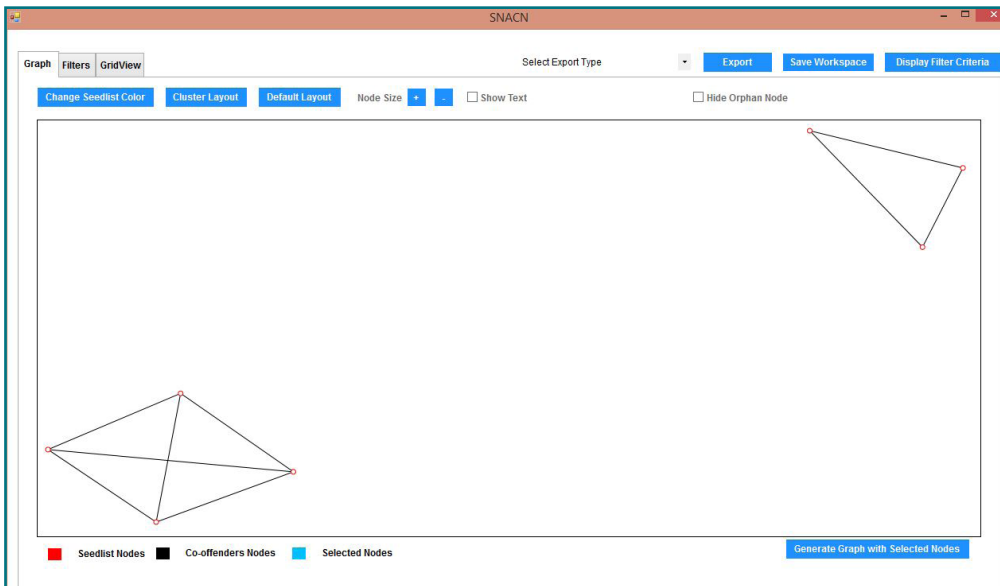
11. Return to the beginning of this section of the lab on loading `Arrest.csv` files to NAVCAP, and try uploading a larger sample dataset with the `Arrest.csv` file located in the `Cooffending` subfolder. After successfully loading the data, generate the graph and you should get a larger network similar to the screenshot below.
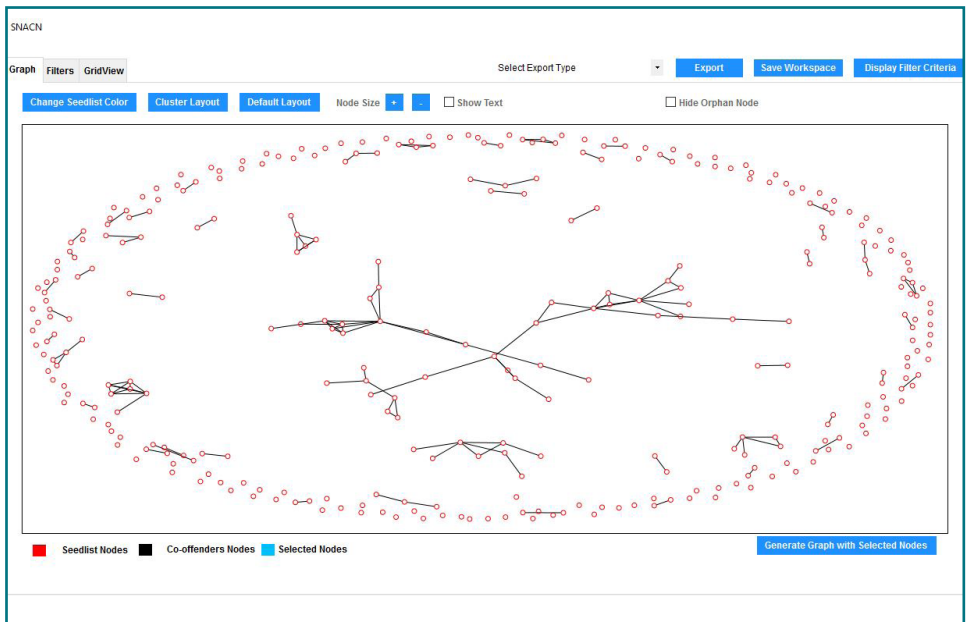
What do you notice in this network at first glance? What might you want to learn to do with this network?

Troubleshooting Arrest.csv

If the `Arrest.csv` file contains mistakes, it cannot upload to NAVCAP properly. You might see a pop-up window like the one below.
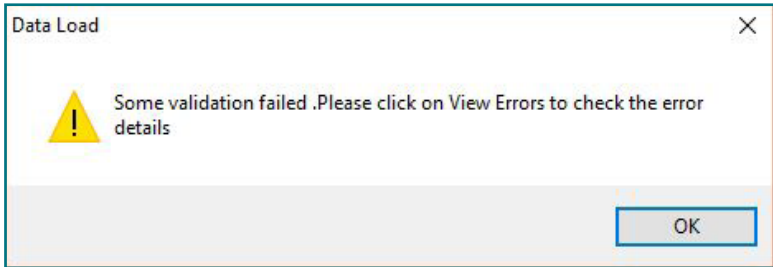
Click on the `OK` button to return to NAVCAP without the upload. Notice the new blue `View Errors` button that appears in the NAVCAP session.
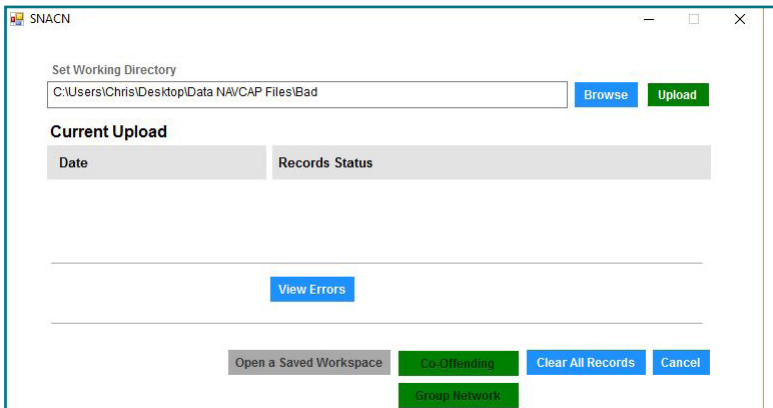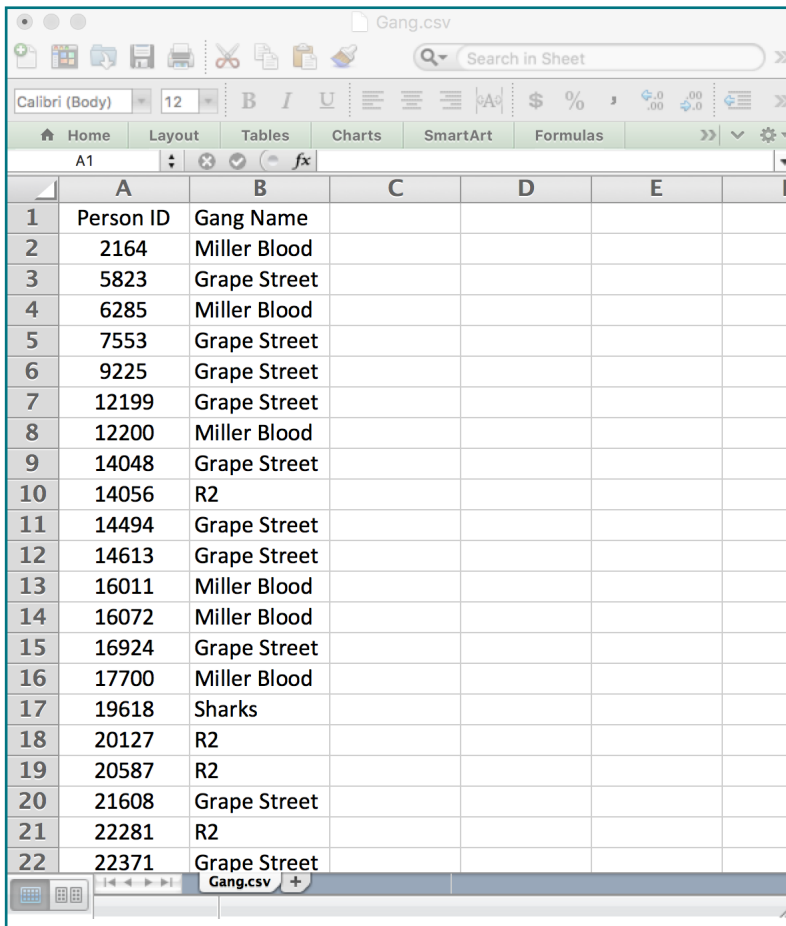
Click on the blue `View Errors` button to open a CSV file that includes some description of what could be going wrong with the `Arrest.csv` file. In the example below, the headers did not match the required file headers. By repairing the headers to match the requirements and saving the `Arrest.csv` file, you can successfully upload this file. Make sure to close the errors Excel file before returning to NAVCAP.
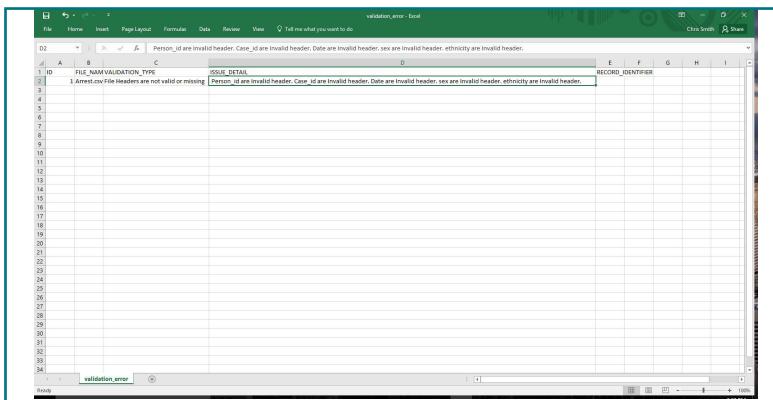
Optional Data Files

Three optional files can be uploaded to NAVCAP that can be linked to the `Arrest.csv` file through the Person ID variable so long as all of the files are contained in the same subfolder. These optional files allow variations to the analysis of the networks. You can build your own version of these files by cutting and pasting your own data into the spreadsheets provided in the `Cooffending` subfolder and saving them as new files in a separate subfolder, like the `Yours` subfolder.

(1) **Gang.csv** ~ a CSV file containing the unique Person ID for someone in the `Arrest.csv` file along with the name or numeric identifier of that person's gang affiliation.
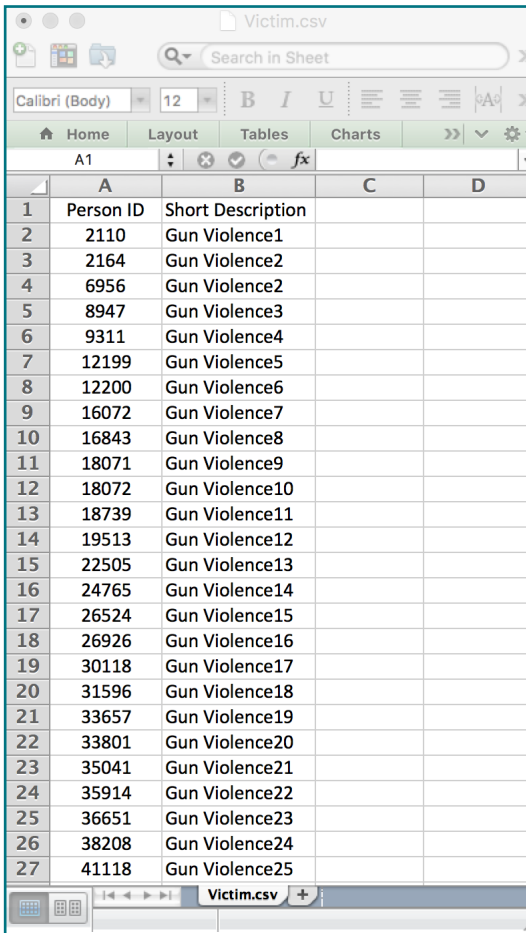
	A	B	C	D	E	F
1	Person ID	Gang Name				
2	2164	Miller Blood				
3	5823	Grape Street				
4	6285	Miller Blood				
5	7553	Grape Street				
6	9225	Grape Street				
7	12199	Grape Street				
8	12200	Miller Blood				
9	14048	Grape Street				
10	14056	R2				
11	14494	Grape Street				
12	14613	Grape Street				
13	16011	Miller Blood				
14	16072	Miller Blood				
15	16924	Grape Street				
16	17700	Miller Blood				
17	19618	Sharks				
18	20127	R2				
19	20587	R2				
20	21608	Grape Street				
21	22281	R2				
22	22371	Grape Street				

This screenshot image is of the `Gang.csv` file located in the `Cooffending` subfolder with the files for this Module 2 lab. Each Person ID in the `Gang.`

csv matches a Person ID from the `Arrest.csv` file located in the shared `Cooffending` subfolder. Gang names are entered here as descriptive names, though these could be unique numeric codes rather than names.
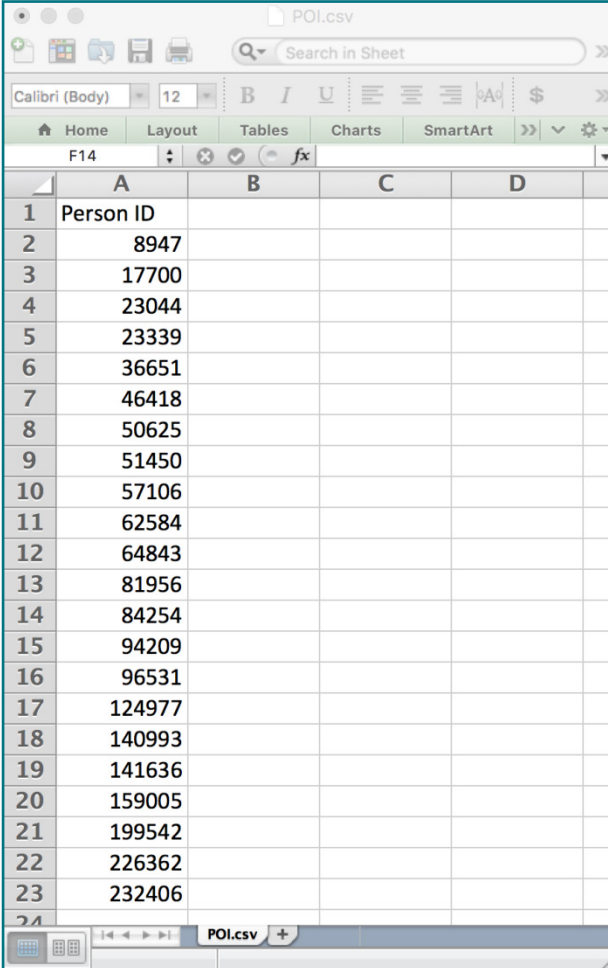
(2) **Victim.csv** ~ a CSV file containing the unique Person ID for someone in the `Arrest.csv` file and some information on the type of victimization or injury that person received—for example, homicide or nonfatal shooting victim.

	A	B	C	D
1	Person ID	Short Description		
2	2110	Gun Violence1		
3	2164	Gun Violence2		
4	6956	Gun Violence2		
5	8947	Gun Violence3		
6	9311	Gun Violence4		
7	12199	Gun Violence5		
8	12200	Gun Violence6		
9	16072	Gun Violence7		
10	16843	Gun Violence8		
11	18071	Gun Violence9		
12	18072	Gun Violence10		
13	18739	Gun Violence11		
14	19513	Gun Violence12		
15	22505	Gun Violence13		
16	24765	Gun Violence14		
17	26524	Gun Violence15		
18	26926	Gun Violence16		
19	30118	Gun Violence17		
20	31596	Gun Violence18		
21	33657	Gun Violence19		
22	33801	Gun Violence20		
23	35041	Gun Violence21		
24	35914	Gun Violence22		
25	36651	Gun Violence23		
26	38208	Gun Violence24		
27	41118	Gun Violence25		

This screenshot image is of the `Victim.csv` file located in the `Cooffending` subfolder with the files for this Module 2 lab. Each Person ID in the `Victim.csv` matches a Person ID from the `Arrest.csv` file located in the shared `Cooffending` subfolder. The second column has the heading Short Description and identifies various injuries or victimization events.

(3) **POI.csv** ~ a CSV file containing the unique Person ID for someone in the `Arrest.csv` file who is of interest to the user or network analyst—for example, an individual who is part of a current violence prevention or intervention effort.

This screenshot image is of the `POI.csv` file located in the `Cooffending` subfolder with the files for this Module 2 lab. Each Person ID in the `POI.csv` matches a Person ID from the `Arrest.csv` file located in the shared `Cooffending` subfolder. This file contains only a single column of Person IDs. This list would only include the Person ID numbers that you are interested in locating within the networks for a particular analysis. If you had a very large network with thousands of nodes, you could upload a `POI.csv` and use it as a filter to zoom in on just the nodes of interest and their connections rather than having to find the nodes manually among the thousands of other nodes.

All three of these optional files will automatically upload along with the `Arrest.csv` file into your NAVCAP session so long as they are all located in the same subfolder and have the correct files names and formatting. Try uploading the `Arrest.csv` file and the accompanying three optional files all located in the `Cooffending` subfolder for this Module 2: Data NAVCAP Lab. You will see that the number of records under Records Status matches the content of the csv files that we viewed in Excel.
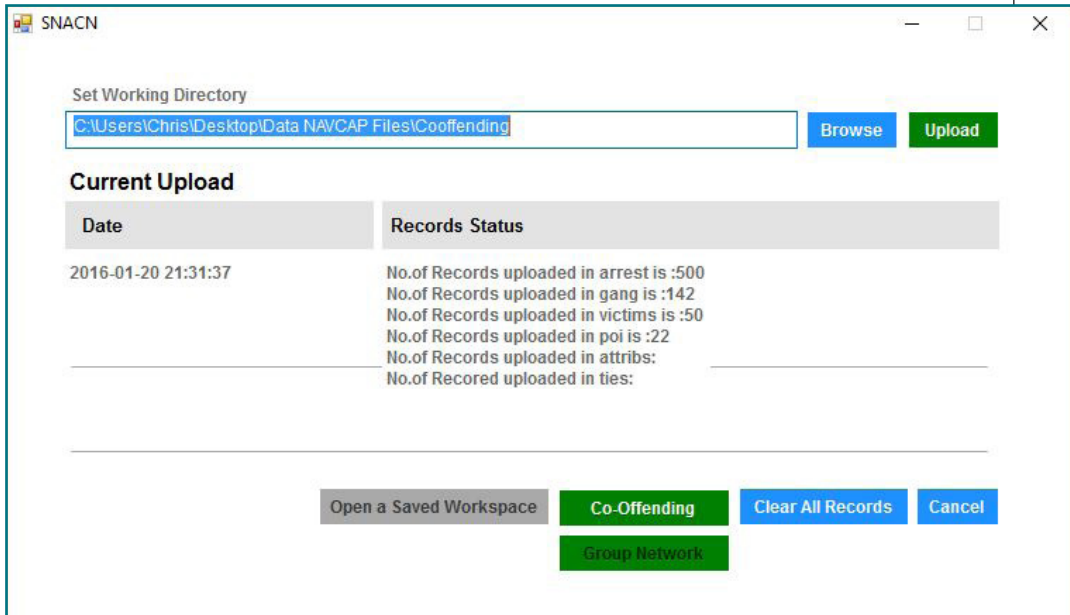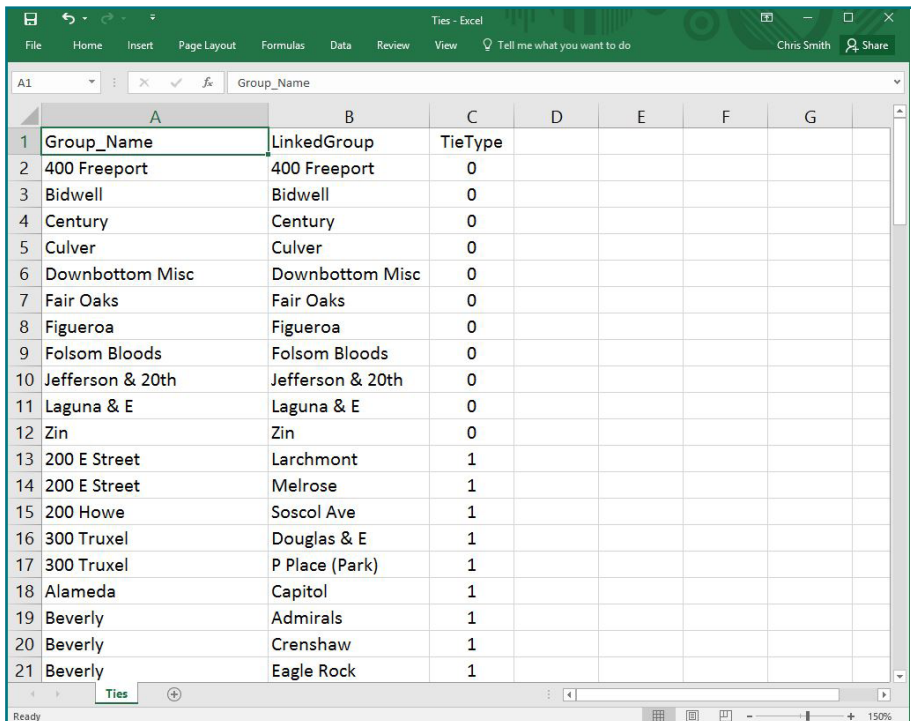
We will cover using these optional files as filters more extensively in Module 4: Analytics.

Group Network

Another functionality in the NAVCAP software is an analysis of relationships between groups. This is a one-mode data option in which the nodes are gangs or groups, and the ties are different types of relationships between those groups, such as alliances or feuds. This information often comes from gang or group audits and can be useful in violence prevention efforts. The group network analysis requires two CSV files with the file name `Ties.csv` and `Attribs.csv`. The `Ties.csv` file links the different groups to each other, and the `Attribs.csv` includes additional information about the groups identified in the `Ties.csv` file. The files for the group analysis are located in the `Group` subfolder. The group analysis is completely separate from the co-offending networks we made with the `Arrests.csv` files.

(1) **Ties.csv** ~ a CSV file linking gangs or groups by different types of relationships. The unique identifiers for the gangs/groups can be descriptive names or alphanumeric identifiers, so long as the same identifier is consistently applied to its group. `Ties.csv` files require 3 exact headers: Group_Name, LinkedGroup, and TieType. The third column, TieType, identifies the different types of relationships that can exist between the groups: 0 = internal ties, 1 = alliances, 2 = feuds, and 3 = volatile. It is worth noting that errors can occur within the NAVCAP software if the headers of the `Ties.csv` are not entered exactly to these specifications.

The screenshot image is of the `Ties.csv` file located in the `Group` subfolder with the files for this Module 2 lab. Groups or gangs are connected in a single row, and are identified by the Group_Name and LinkedGroup columns. The different types of relationships are identified by the TieType identifier also included in each row. Because the nodes are groups in this type of NAVCAP analysis, it is possible that some of these relationships exist within the groups. Notice how the top rows in this screenshot have the same group name in the Group_Name column as well as the LinkedGroup column. We can see from the zeros in the TieType column that these are internal relationships within the group. In the network, we expect these specific ties that are equal to 0 to form small loops attached to particular nodes.

(2) **Attribs.csv** ~ a CSV file with more detailed information about each gang or group. The `Attribs.csv` file links to the unique group names or identifiers in the `Ties.csv` file. Note: isolate groups (groups that do not have any ties, feuds, or alliances with other groups) should be entered in the `Attribs.csv` file, if you have them. If you enter them in `Ties.csv` without a linked group, they are automatically given an internal tie. It is important to point out that you can have more groups in attribs.csv than ties.csv, but not less.

The `Attribs.csv` file provides additional information to the `Ties.csv` file that can be analyzed in the NAVCAP application. The `Attribs.csv` file requires the following 4 exact headers: Name (which must match the group names or identifiers from the `Ties.csv`), District, Race, and Status.


	A	B	C	D
1	Name	District	Race	Status
2	Capitol	D8	B	active
3	Folsom Bloods	D8	B	active
4	200 Howe	D8	B	active
5	Fair Oaks	D10	B	active
6	400 Freeport	D8	B	active
7	300 Truxel	D4	B	active
8	El Camino	D8	B	active
9	Burn Boys	D9	B	inactive
10	Zin	D8	H	active
11	Sunrise Crew	D3	B	inactive
12	Laguna & E	D4	B	active
13	Douglas & E	D4	B	inactive
14	Bidwell	D8	B	active
15	Iron Point	D4	B	inactive
16	Downbottom Misc	D4	B	active
17	Common Bloods	D7	B	inactive
18	Monte Vista	D9	B	active
19	Tienda	D9	B	inactive
20	Century	D8	B	active
21	Soscol Ave	D9	B	inactive

This screenshot image is of the `Attribs.csv` file located in the `Group` subfolder with the files for this Module 2 lab. The Name column matches the group names used in the `Ties.csv` file. The remaining three columns (District, Race, and Status) include other useful information collected and/or organized by the analyst. Importantly, the Status column must have either "active" or "inactive" entered in lower case.

Return to your NAVCAP session. Click on the blue `Clear All Records` button. Once the files are cleared, then click on the blue `Browse` button to change the working directory to the `Group` subfolder where the `Ties.csv` and `Attribs.csv` are located. Then click on the green `Upload` button.
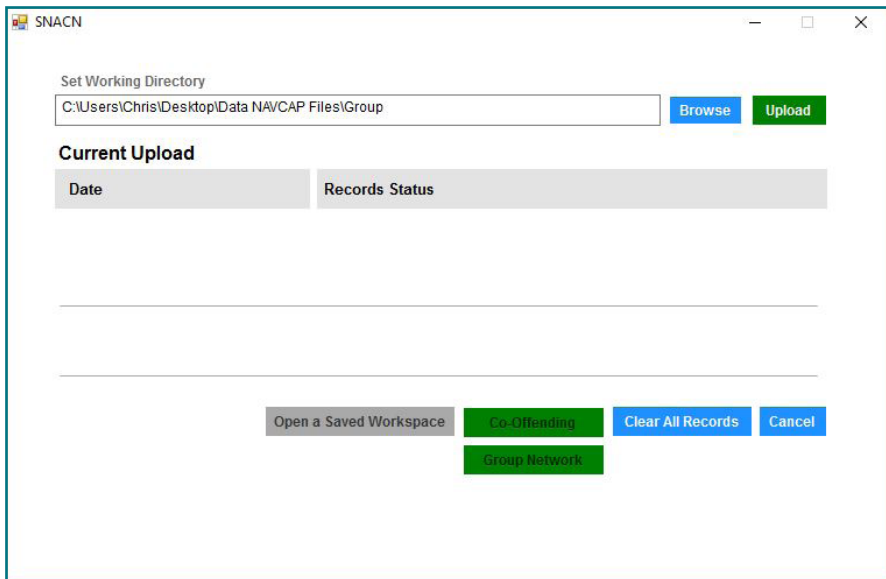
You will receive a message in the File Upload Status window stating that the `Ties.csv` and `Attribs.csv` are valid, but that an arrest file is needed. Remember how earlier we learned that the `Arrest.csv` is the main file for the NAVCAP software. However, in the case of the group network, we do not need the `Arrest.csv` file, because it has no connection to the group analysis. Click `OK` on this message box.
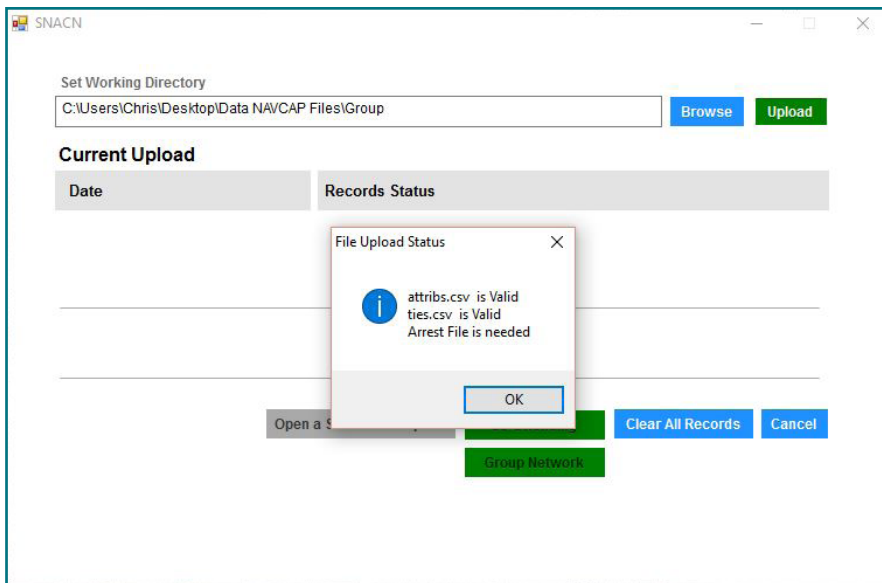
In its current version, the NAVCAP program believes that the missing `Arrest.csv` file is an error. If you click on the blue `View Errors` button, a spreadsheet will open explaining the validation issue. However, this does not actually interfere with the group analysis. So long as you have records showing under the Records Status list for `attribs` and `ties,` then you can run the group network. Go ahead and click on the green `Group Network` button toward the bottom of the window. The group network will automatically open. The default colors will differentiate between the different types of ties and the different statuses of the groups.

Network Analysis and Visualization for Crime Prevention (NAVCAP)

Review of Module 2: Data

CSV is a file extension that stands for "comma separated values." A CSV file is essentially a text file in which information is separated by commas. CSV files are versatile files that can be read easily by many software programs that can read text or spreadsheets.

The main file required for the NAVCAP application is the `Arrest.csv` file. Use subfolders for different networks in order to maintain the correct names of the files. There are three optional files that can be linked to the `Arrest.csv` file: `Gang.csv`, `Victim.csv`, and `POI.csv`. You can quickly inspect the entire contents of the `Arrest.csv` file as a co-offending network by clicking on the green `Co-offending` button, including all of the dates in a date range filter, setting the connections to `1` in the Set Seed Filter window, and then clicking the green `Generate Graph` button.
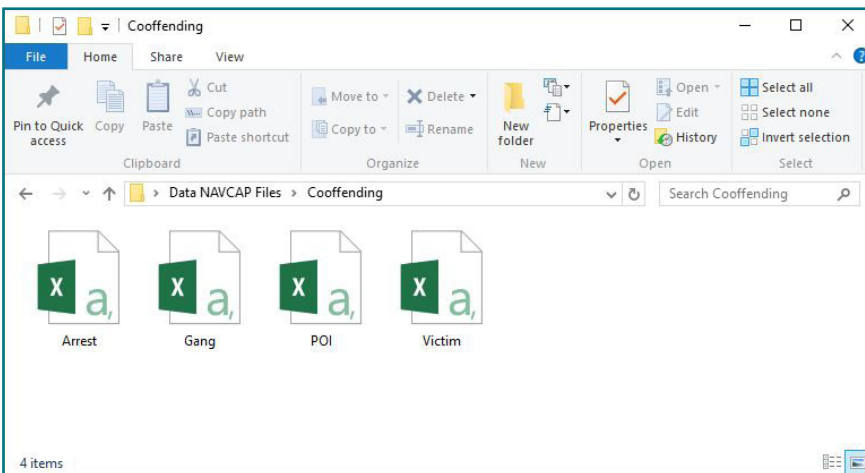
Group analysis is possible using the `Ties.csv` along with the `Attribs.csv`. In its current version, ignore the validation error regarding the `Arrest.csv` file when conducting the group network analysis. The group analysis does not require any filters. Once the two required files are loaded, click on the green `Group Network` button to generate the group network image.
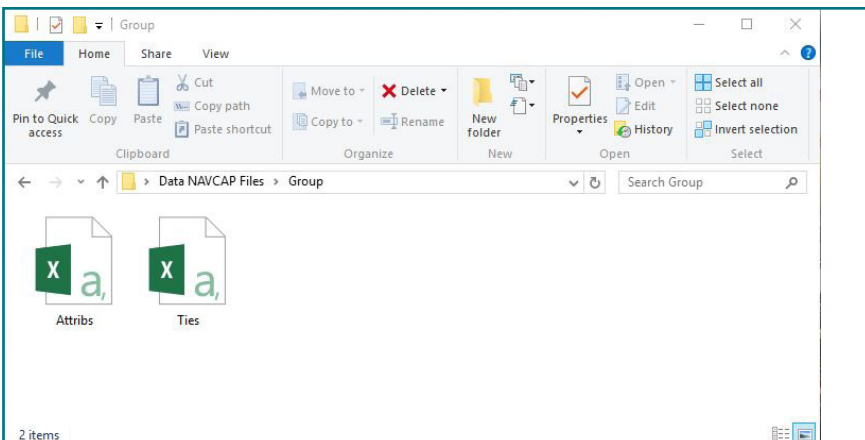
MODULE 3: VISUALIZATION

Goal:

Participants will be introduced to various plotting options in NAVCAP and learn how to customize network images.

Visualization NAVCAP Files
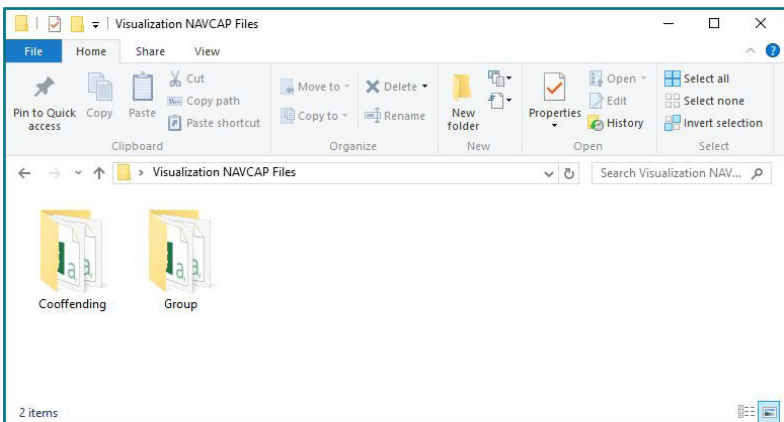
The `Visualization NAVCAP Files` folder contains two subfolders: `Cooffending` and `Group`. These subfolders contain all of the files needed to complete the Module 3: Visualization NAVCAP Lab.

The `Cooffending` subfolder contains four CSV files that can be used in the NAVCAP co-offending networks, and the `Group` subfolder contains two required csv files for the NAVCAP group network.
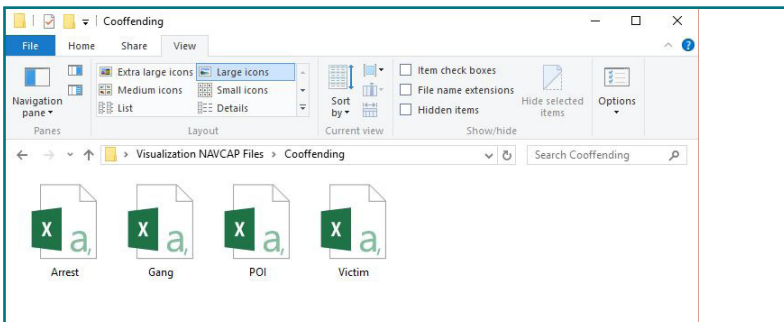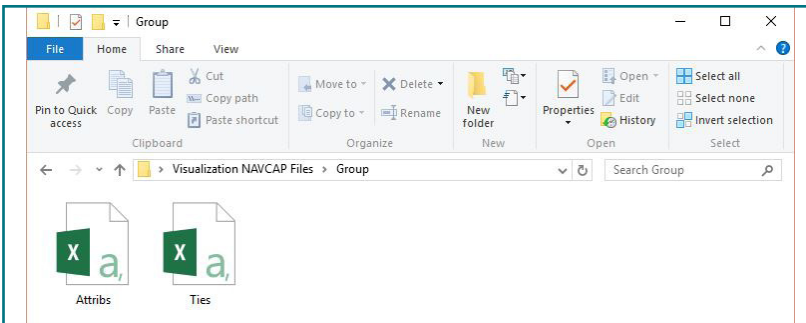
If you need a refresher of what these files look like outside of NAVCAP, you can view the csv files in either a spreadsheet software program or a simple text-editing program.

Visualizing Co-Offending Network
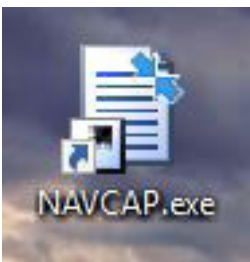

A. Open the NAVCAP application on your computer.

Note: Some of the screenshots for this lab were taken from an earlier version of the NAVCAP application and might not exactly match your screen.

B. Generate a co-offending network image of the sample `Arrest.csv`. For more detailed instructions on steps 1 through 4 below, review the Module 2: Data NAVCAP Lab documents.

1. Set the working directory to the `Cooffending` subfolder located in the `Visualization NAVCAP Files` folder.
2. Upload the data files by clicking on the green `Upload` button.
3. Once the files upload then click on the green `Co-Offending` button.
4. Generate a graph of the entire dataset by selecting 1 under Connections, setting the Arrest Date Range from January 1, 2015 to today's date, and clicking on the green `Generate Graph` button.
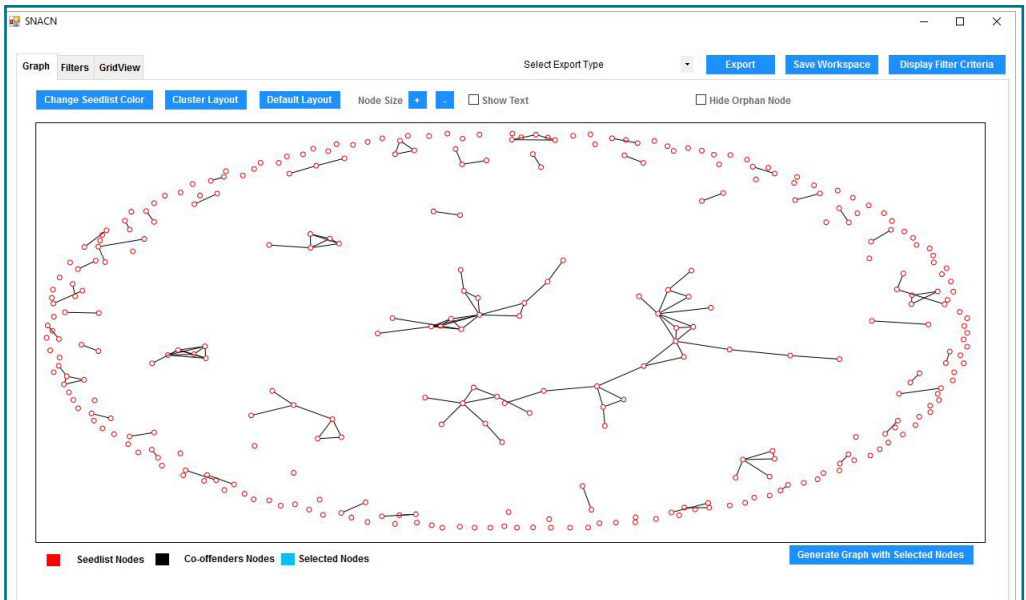
C. Customize the Co-Offending Network.

1. Hide the isolates by checking the box next to `Hide Orphan Node`.

2. Change the layout of the nodes by clicking on the blue `Default Layout` button. You can do this as many times as you want to see the network move around in the plotting space. Alternatively, you can organize the presentation of the network by the different-sized components of the network by clicking on the blue `Cluster Layout` button. The left side of the frame will contain isolates and the right side of the frame will organize the various components.

3. Change the size of the nodes by clicking on the blue plus (+) and minus (–) signs next to `Node Size`.

4. Change the color of the nodes by clicking on the blue `Change Seed List Color` button. Select a color of your choice, and click the `OK` button.

5. Display node labels by clicking on the box next to `Show Text` and selecting either `Person ID` or `Node ID` for the labels to be displayed. The Person ID labels come directly from the Arrest.csv file. The Node ID labels are generated within NAVCAP and number the nodes in the network starting with 0.

6. Zoom in on parts of the network by moving your mouse to the area where you want to zoom in and scroll using your mouse.
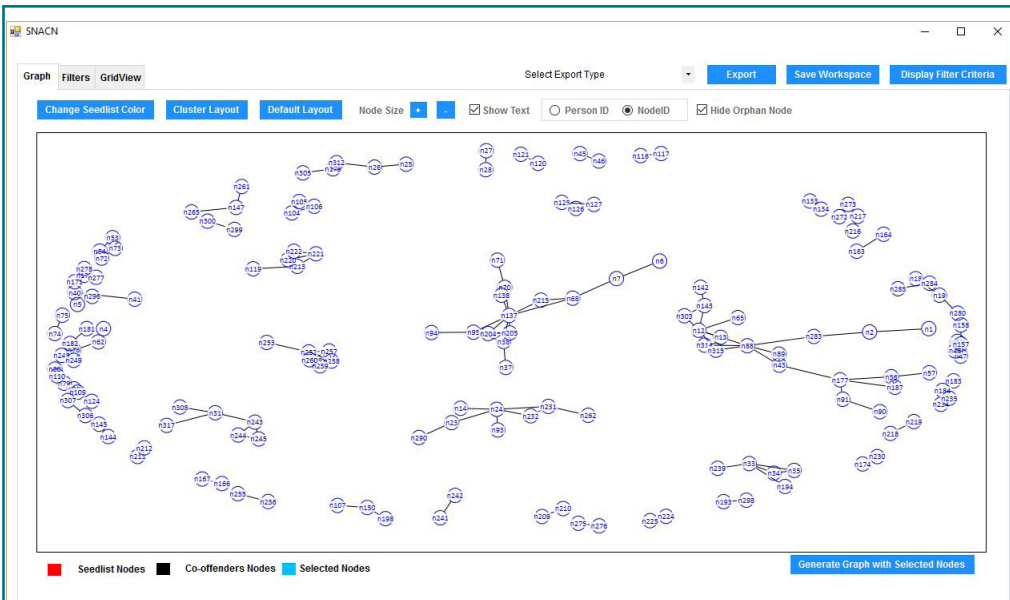
7. Select a node of interest by clicking on it. Select multiple nodes by holding down the control button on your keyboard while clicking on additional nodes of interest. You can also double click to highlight everyone one degree away from the node you click. Triple click to highlight everyone two degrees away, and so forth.

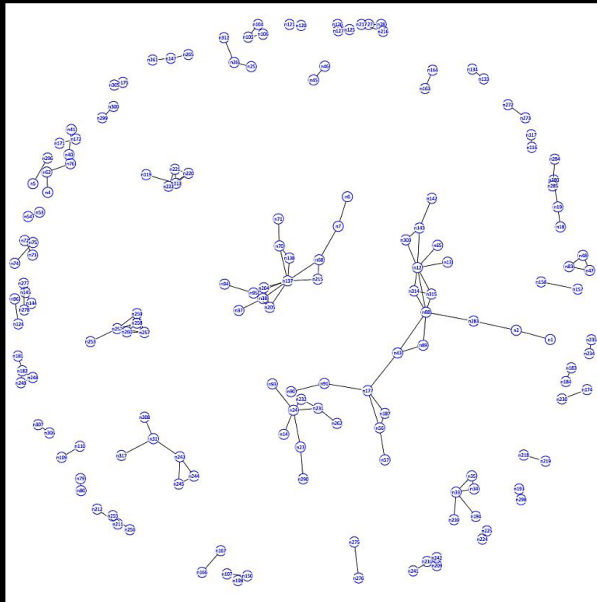You can also draw a box around the desired nodes and select the "generate graph."

Click on the blue `Generate Graph with Selected Nodes` button.
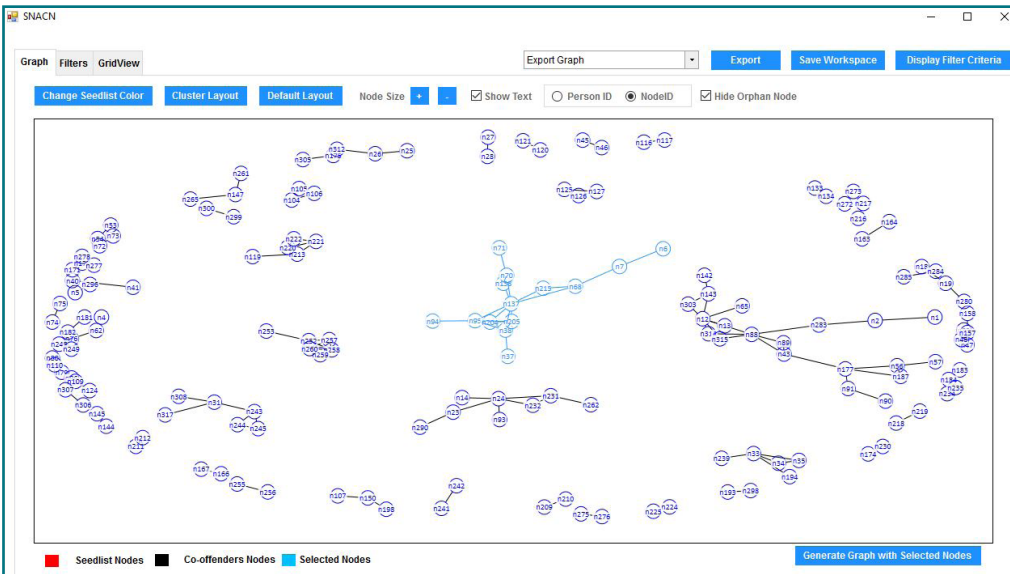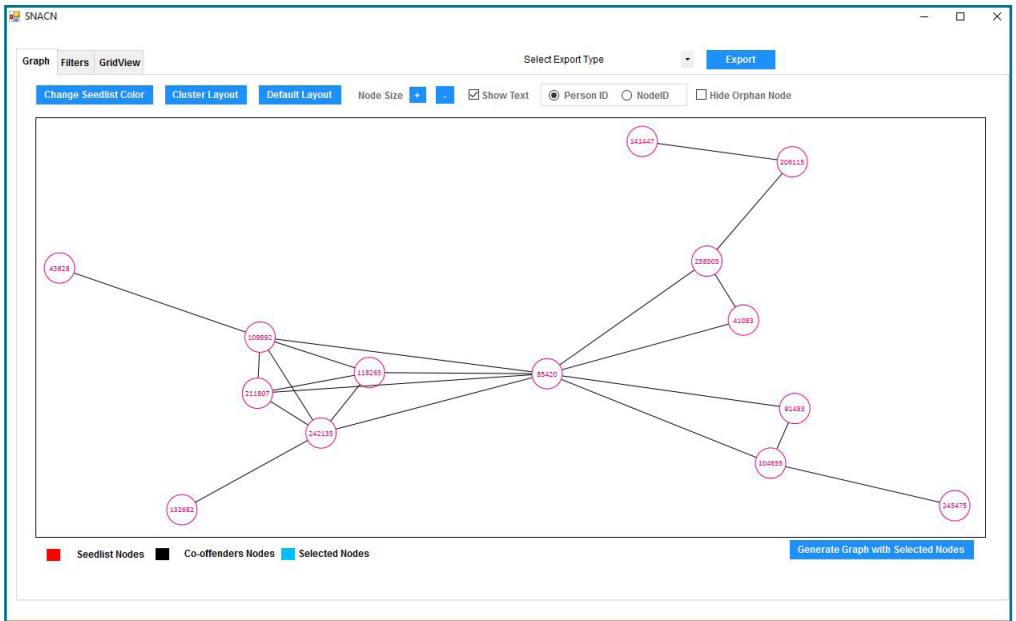
8. You can save any of your network images as a pdf (portable document format) or a png (portable network graphics) file. The `Export Graph` option generates a png file. Select which file type you want to export and then click on the blue `Export` button. This will open a Save As window where you can decide where on your computer you want to save your file and what you want to name your file.

9. Open your network image outside of NAVCAP. In the screenshot example below, the png file was opened with the default Microsoft photo application.

Visualizing Group Network

A. Return to the upload screen of NAVCAP to change the data for a group network.

B. Load the group network files. For more detailed instructions on steps 1 through 3 below, review the Module 2: Data NAVCAP Lab documents.

1. Set the working directory to the `Group` subfolder located in the `Visualization NAVCAP Files` folder.
2. Upload the data files by clicking on the green `Upload` button.
3. Once the files upload, then click on the green `Group Network` button.
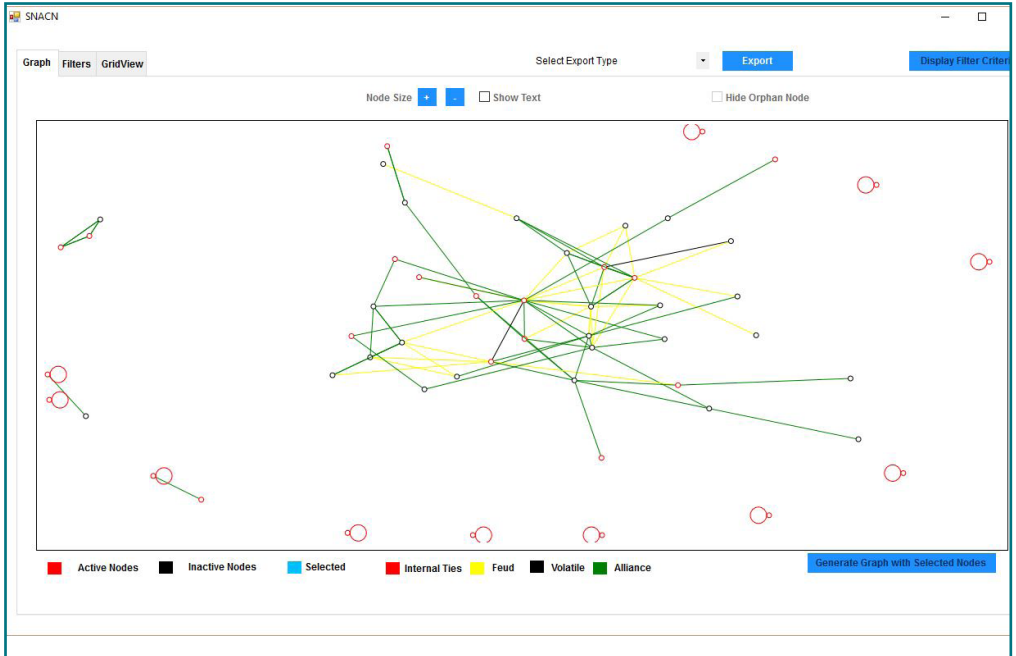
C. The customization options for the group networks are a bit different from the co-offending networks produced in the NAVCAP application. Below are the customization options available for the group network.

1. Change the size of the nodes by clicking on the blue plus (+) and minus (–) signs next to `Node Size`.

2. Display node labels by clicking on the box next to `Show Text`, and selecting either `Person ID` or `Node ID` for the labels to be displayed. The Person ID labels come directly from the `Ties.csv` file. The Node ID labels are generated within NAVCAP and number the nodes in the network starting with 0.

3. Zoom in on parts of the network by moving your mouse to the area where you want to zoom in and scroll using your mouse.

Network Analysis and Visualization for Crime Prevention (NAVCAP)
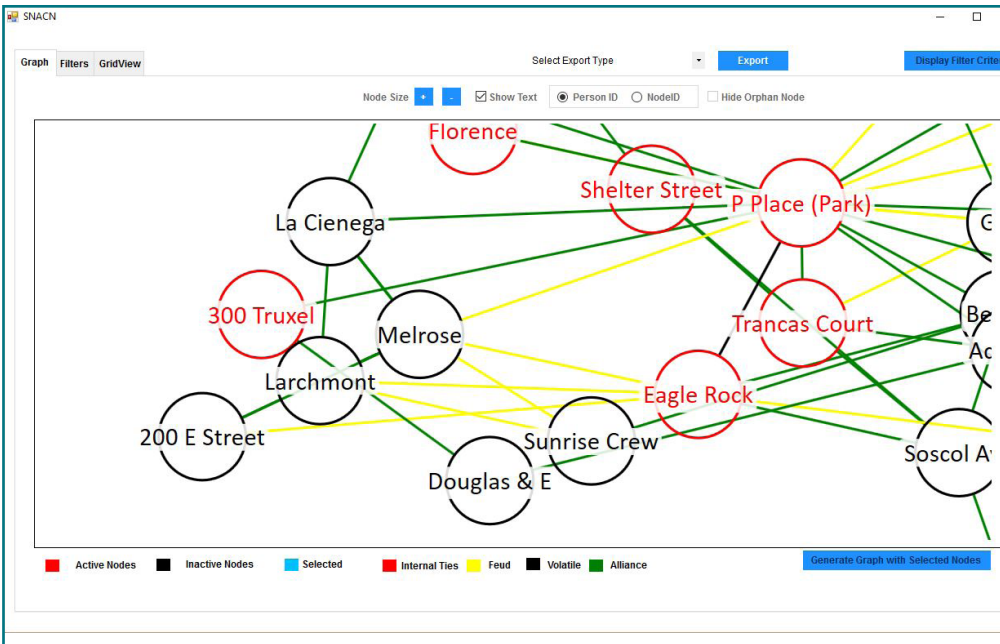
4. To limit the visualization by tie type (internal ties, feuds, volatile, or alliances), click on the `Filters` tab toward the upper left of the visualization window. Under `Ties Type`, you can select `All`, `0` for internal ties (red), `1` for alliances (green), `2` for feuds (yellow), and `3` for volatile (black). Once you select the ties that you want the visualization limited to, click on the green `Apply Filter` button, and then return to the `Graph` tab in the upper left.
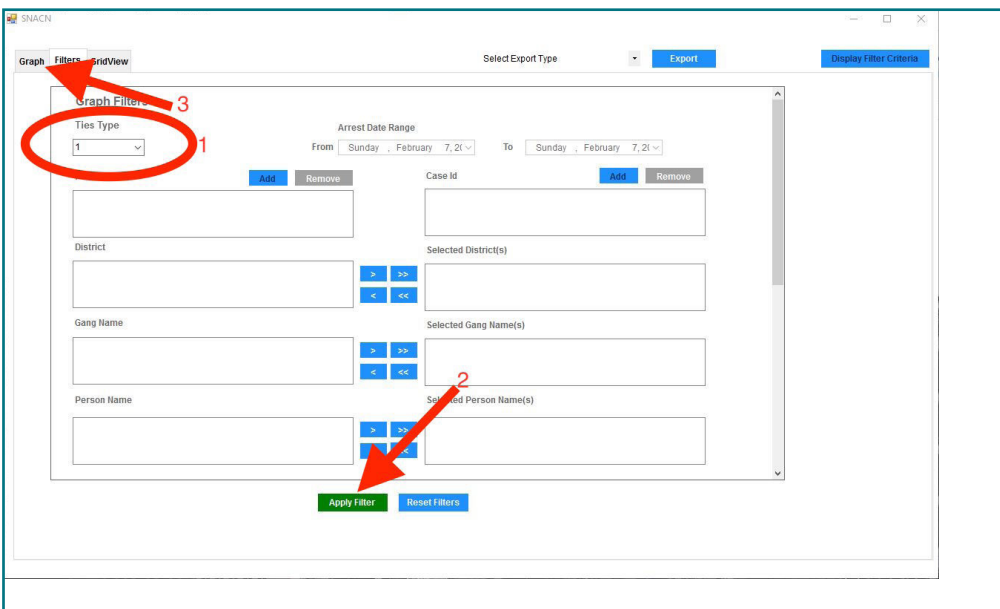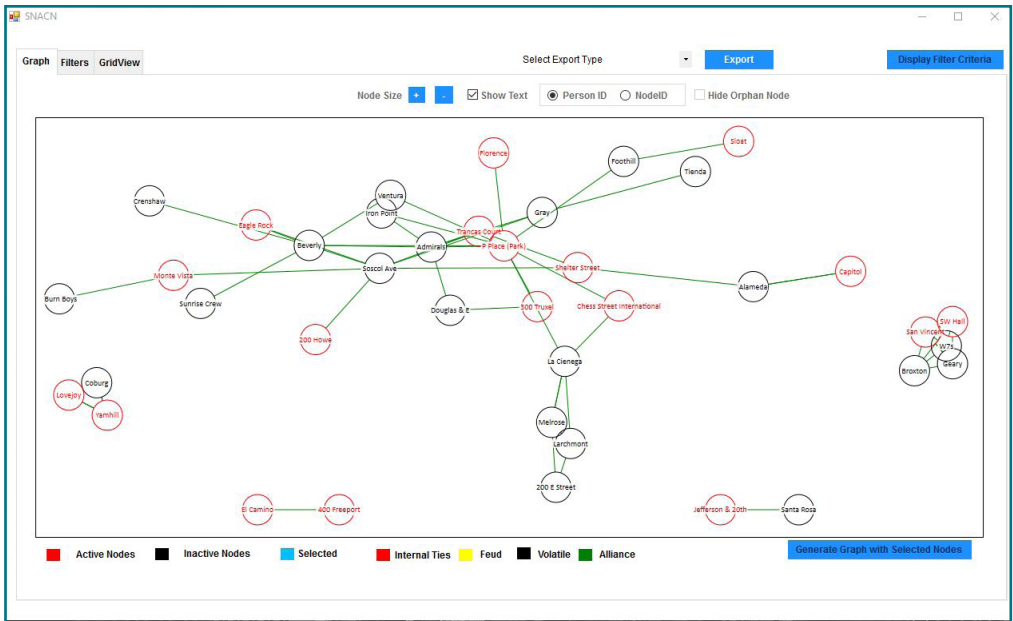
5. Save any of your group networks using the same export function described above.

Review of Module 3: Visualization

There is some variation in the customization options available in the co-offending network and the group network within NAVCAP.

The co-offending network requires filters before generating the graph. Once the graph has been generated, users have control over node labels, node size, isolates, color of nodes, layout, zooming in and out of sections of the figure, and selecting nodes to create a smaller version of a network.

The group network produces the network image without entering filters. Users do not have control over colors used in the network, but users do have the option of examining only one type of relationship. Users can change the labels and node size in group networks. Once the network image is available, users can place their cursor on a section of the network and scroll in to zoom.

MODULE 4: ANALYTICS

Goal:

This lab introduces participants to the filter options and neighborhoods to analyze co-offending networks in NAVCAP.
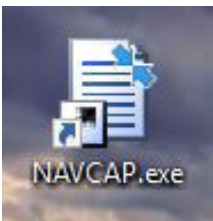
Analytics NAVCAP Files
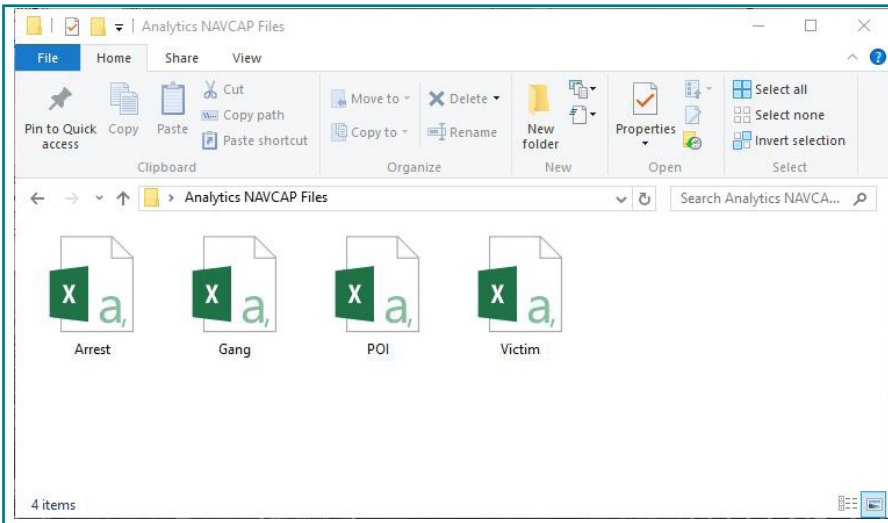
The `Analytics NAVCAP Files` folder contains four csv files connected to the co-offending networks in NAVCAP. Participants learned about these files in Module 2.

Note: At the time of this writing, there were no additional options available for analyzing the group network, so this lab is limited to the analytics available for the co-offending network.
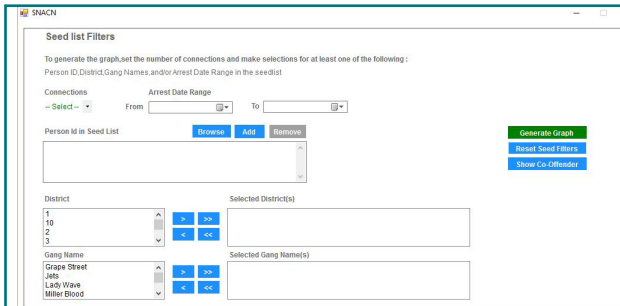
1. Start by opening the NAVCAP application on your computer.

Note: Some of the screenshots for this lab were taken from an earlier version of the NAVCAP application and might not exactly match your screen.

2. Set the working directory to the `Analytics NAVCAP Files` folder.
3. Upload the data files.
4. Proceed to the co-offending network.

Person ID Seed List Filters

One of the csv files located in the `Analytic NAVCAP Files` folder is the `POI.csv`. Recall from Module 2: Data that this CSV file includes a hypothetical list of persons of interest. The `POI.csv` files contains nothing more than 22 Person IDs that match Person IDs in the `Arrest.csv` file. Let's assume that we are interested in all of the individuals on this person of interest list for a wellness check, and we need to know to whom they are connected in case we have trouble locating them. In order to do this, we need to open the POI file in the Person ID Seed List.

1. Click on the blue `Browse` button next to the `Person ID Seed List`.
2. Locate the `POI.csv` file in the `Analytic NAVCAP Files` folder, and click `Open`.
3. Select `1` under `Connections`.
4. Click on the green `Generate Graph` button.

The red nodes in the network image are the 22 nodes identified in the `POI.csv`, and the black nodes are the direct co-offenders to the nodes of interest who were not on the POI list. Not every person of interest had a direct co-offender, but all of the relationships between this reduced set of nodes are displayed in this network.
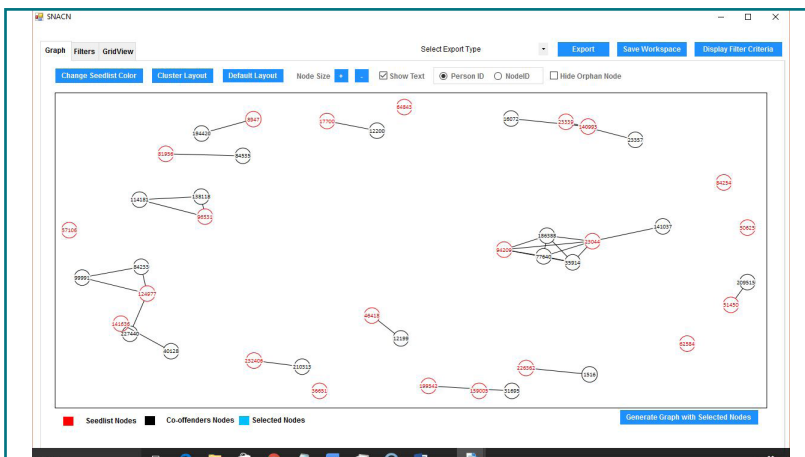
5. Click on the `Grid View` tab in the upper left of the window to display a table of just the nodes included in the POI network.

|	Select		Node ID	Person ID	Case ID	District	Gang Name	Person Name	Age	Gender	IsVictim	Victim Description
▶	☐	...	n0	17700	320670,17730...	5,5,10,5	Miller Blood			M	No,No,No,No	
	☐	...	n1	40128	369285,16810...	1,1,1,8	Sharks			F	No,No,No,No	
	☐	...	n2	51450	374265	2				F	No	
	☐	...	n3	209515	374265	2				F	No	
	☐	...	n4	57106	385875	2				M	No	
	☐	...	n5	124977	416538,1241373	2,2	Grape Street			M	Yes,Yes	Gun Violence4...
	☐	...	n6	227440	416538	1	Grape Street			M	No	
	☐	...	n7	210313	468468	5	R2			M	No	
	☐	...	n8	232406	468468	5	R2			M	No	
	☐	...	n9	62584	483672	5				M	No	
	☐	...	n10	96531	614907	8				M	No	
	☐	...	n11	114181	614907	8				M	No	
	☐	...	n12	138118	614907	8				M	No	
	☐	...	n13	84254	631698	4				F	No	
	☐	...	n14	31695	871584,94725...	7,7,7,7,7,2				M	No,No,No,No,N...	
	☐	...	n15	159005	981876,2016888	5,5				M	No,No	
	☐	...	n16	64843	996936	10				F	No	
	☐	...	n17	50625	1001022	3				M	No	
	☐	...	n18	140993	1111350,12669...	8,8,8,8	Miller Blood			F	Yes,Yes,Yes	Gun Violence4...
	☐	...	n19	84233	1161468,1241...	2,2,2,2,3,2	Miller Blood			F	No,No,No,No,N...	
	☐	...	n20	99991	1241373	2	Miller Blood			F	No	
	☐	...	n21	1516	1382460	8				F	No	
	☐	...	n22	226362	1382460	8				F	No	

You can export just this table by selecting `Export Data Excel (All Nodes)` next to the blue `Export` button, or you can click some of the boxes on the far left of the to export a further reduced table of selected nodes.

Selected District and Gang Filters

The `Arrest.csv` for this module includes a district column for where each arrest event occurred. You can limit your co-offending network to just the nodes arrested within selected districts and their associates.

1. Reset the Seed List Filter window by clicking on the blue `Reset Seed Filters` button.
2. Select the district of interest and click on the blue arrow (`>`) to move that particular district to the `Selected District(s)` box.
3. Select `1` under `Connections` to include only the nodes directly connected to those arrested in the selected district.
4. Click on the green `Generate Graph` button.

Below is the network of the red nodes arrested in district 9. The black nodes are their associates who were connected to them in co-arrests outside of district 9.
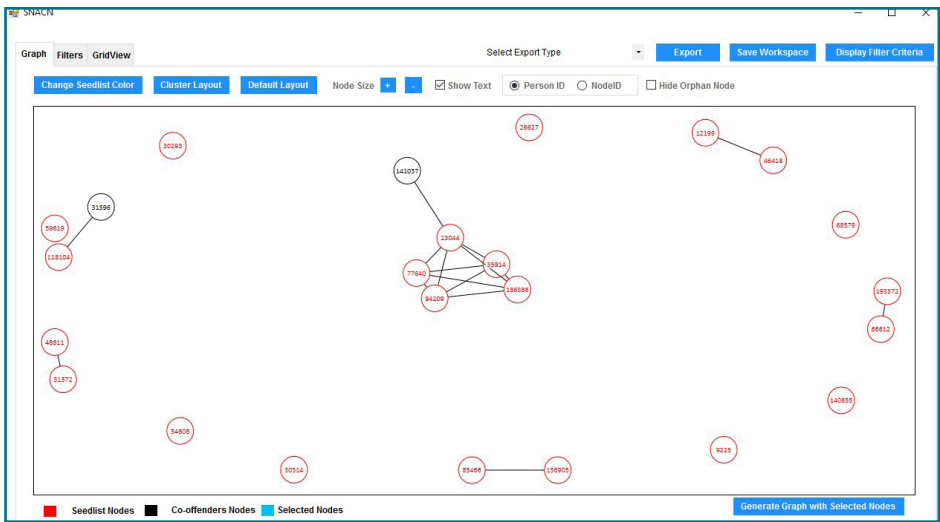
Analyzing particular gangs requires the same process as analyzing districts, but the gang names are imported from the Gang.csv located in the Analytic NAVCAP Files folder. Let's analyze the relationships between the Miller Blood gang and the R2 gang.

1. Click on the blue Reset Seed Filters button to begin a new analysis.
2. Select Miller Blood and R2 from the Gang Name box and click the blue arrow pointing right (>) to move these two gangs to the Selected Gang Name(s) box.
3. Select 1 under Connections.
4. Click on the green Generate Graph button.

Again, the default red nodes are the nodes identified through the gang filter. These nodes are also the nodes that you can adjust the colors for, such as orange. The black nodes, which you cannot adjust the colors for, are the nodes that are directly connected to the Miller Blood and R2 gang nodes but are not part of those selected gangs.

Network Analysis and Visualization for Crime Prevention (NAVCAP)
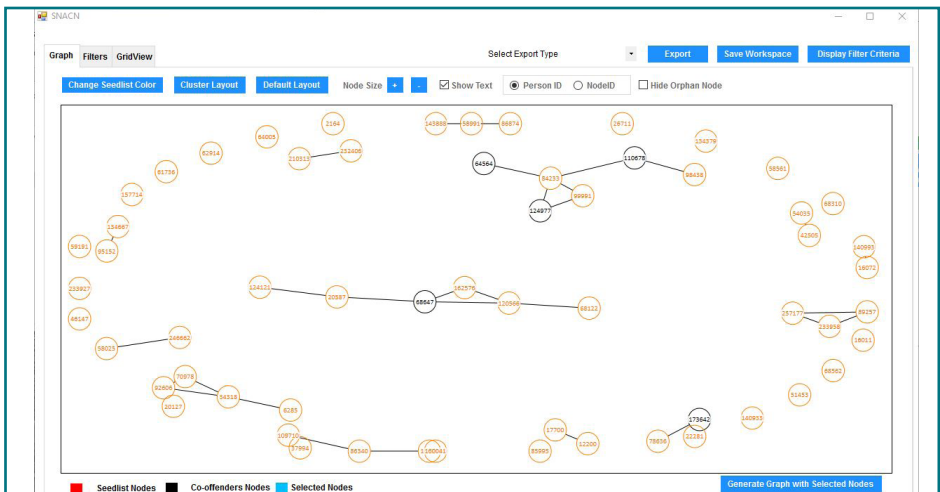
Show Co-offender Filters

Return to the `Seed List Filters` window, and you will see a blue `Show Co-Offender` button on the right. Click on this button to open another panel of filters. This panel gives you more analytic options to generate networks based on certain attributes. The `Show Co-Offender` button changes to a `Hide Co-Offender` button when the bottom panel is open.


To create a network based on a set of attributes, first set the upper panel to include all of the nodes and ties in the `Arrest.csv` file by following steps 1 through 3 below.

1. Click on the blue `Reset Seed Filters` button to begin a new analysis.
2. Select `1` under `Connections`.
3. Either select all of the Districts (use the blue double right arrow button `>>`) or enter the date range from January 1, 2015 to today's date.

These first three steps will select all of the nodes and ties for this particular `Arrest.csv` file, and from there we can set filters to analyze particular attributes from the `Show Co-offender` panel. Notice that you have access to the `Victim.csv` file that we examined in Module 2, which was a list of Person IDs who had been hypothetical victims of violence. This is our first time using the `Victim.csv` file in these training materials.

4. Select that various attributes of interest and then generate the graph. If you don't want the attributes to cumulate, clear them with the blue `Reset Co-offender` button in the lower panel.

Here is a network of just the 76 women in the co-offending network and the relationships between them.
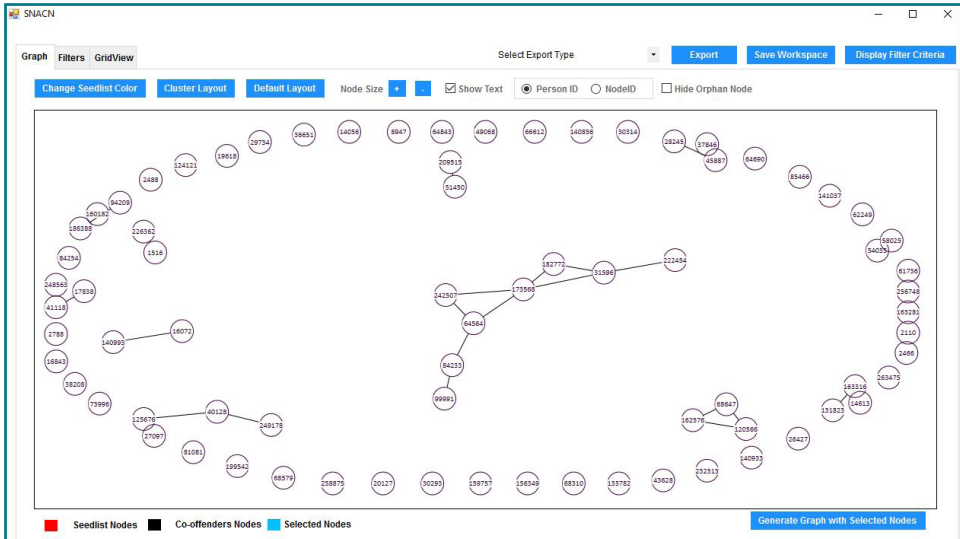
Here is a network of just the 50 nodes who were victims as identified in the `Victim.csv` file and the relationships between them according to the `Arrest.csv` file.
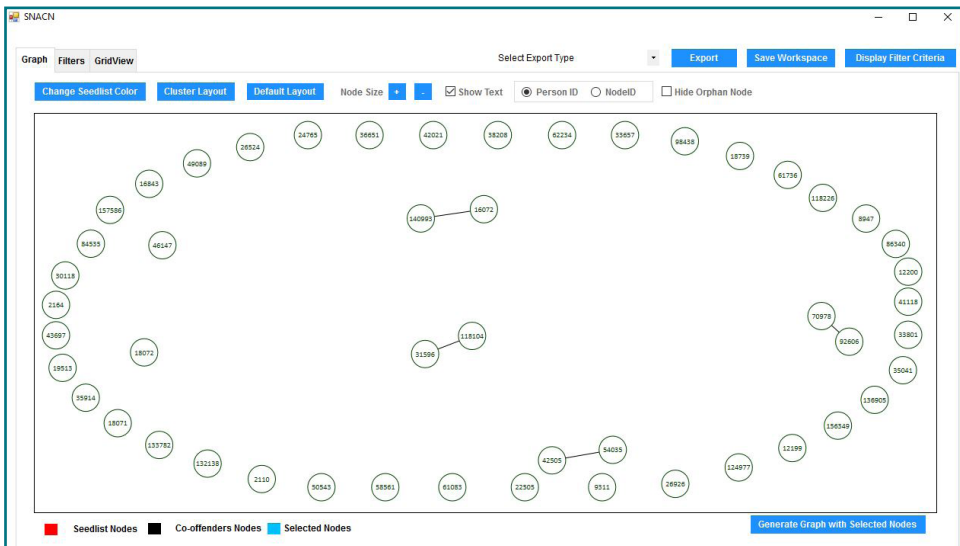
Neighborhood Analysis

Beyond the filtering options, NAVCAP has one feature for analytics. We can use the different numbers for `Connections` to conduct a neighborhood analysis. Recall that a neighborhood refers to the "alters" (e.g., a node is connected to a particular node of interest) within a specific distance (e.g., 1, 2, 3, etc.) from a focal node, also called a "node of interest" or an "ego." Selecting `1` under `Connections` produces a first order neighborhood from the ego. Selecting `2` under `Connections` adds the nodes that belong to the second order neighborhood, and so on.

Generate the different neighborhoods for Person ID 31596. This node is well-connected in one of the larger components and provides a good visual for neighborhood analysis within this co-offending network.

1. Return to the `Seed List Filter` screen and click on the blue `Reset Seed Filters` button to begin a new analysis. Also clear the lower panel by clicking on the blue `Reset Co-offender` button.
2. Type in the Person ID for the node of interest, 31596, in the `Person ID` in the `Seed List` box.
3. Select `1` under `Connections`.
4. Click the green `Generate Graph` button.

Note that the ego, #31596, is in the middle of the network and is a different color than the other nodes (alters) in the first order neighborhood. There are a total of 8 nodes in this first order neighborhood. If you do not want to count the nodes manually, just click on the `Grid View` tab to see the Node IDs newly generated in numerical order for just this small network.
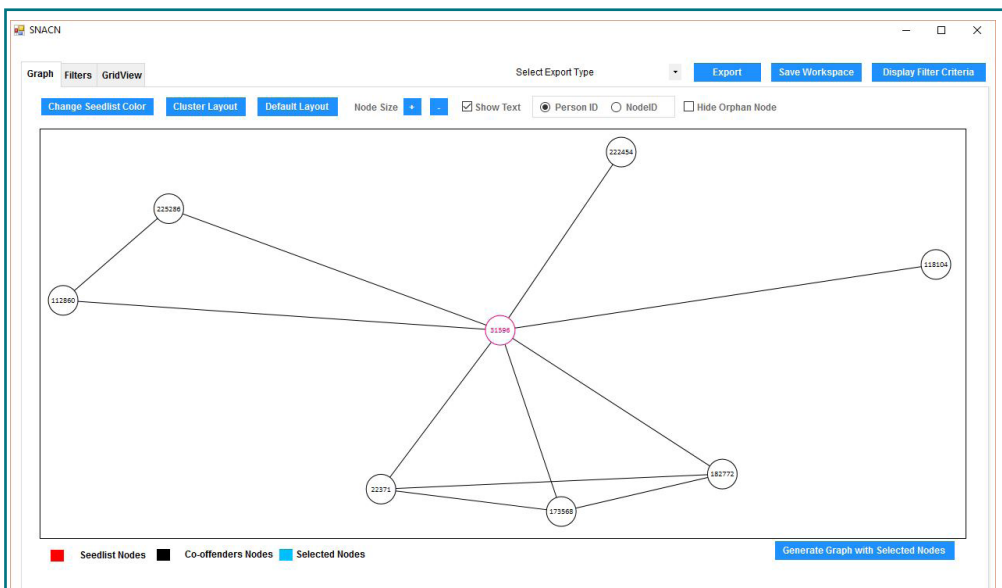
5. Close the first order neighborhood network to return to the `Seed List Filters` screen.
6. Change the `Connections` to `2` to generate a second order neighborhood for node 31596.
7. Click on the green `Generate Graph` button.

Now there are 12 nodes in the network, and we can see nodes connected to the ego's alters. The node of interest is no longer directly connected to all of the alters, but this second order neighborhood network includes all nodes that are within two links of the ego.
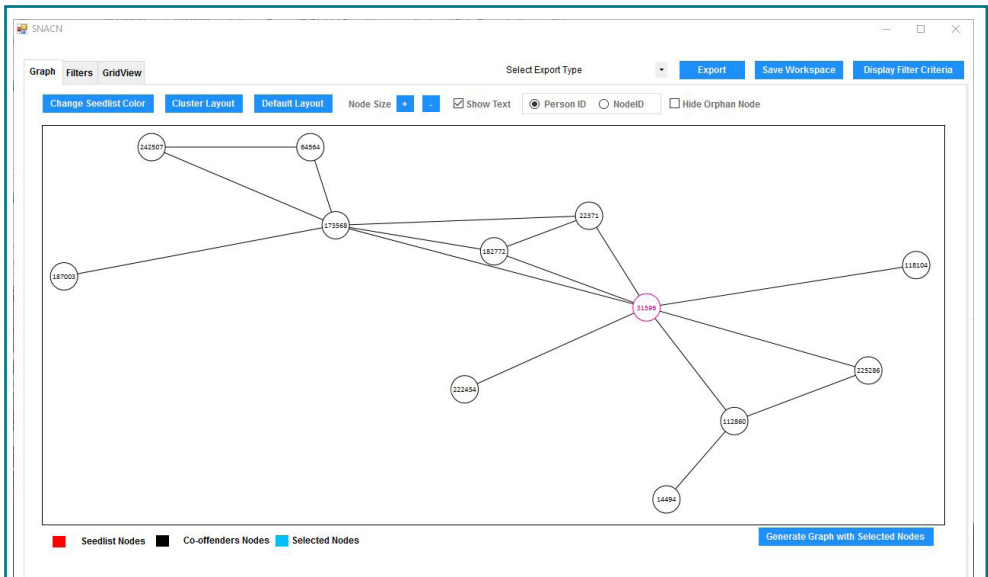
Repeat these steps to generate the third, fourth, and fifth order neighborhoods. At the higher orders, you will notice that the ego moves farther to the edges of the component rather than being centrally located in the component.

Network Analysis and Visualization for Crime Prevention (NAVCAP)

Review of Module 4: Analytics

In their current form, analytics are limited to the co-offending networks and not available for the group networks in the NAVCAP application.

Some of the analytic possibilities for the co-offending networks in NAVCAP include:

~ Filtering your network based on Person IDs either through a `POI.csv` file or by manually entering the Person ID numbers.

~ Filtering your network based on District.

~ Filtering your network based on Gang.

~ Filtering your network based on some other attribute variable, such as victim or gender.

~ Use the `Grid View` to analyze the tables generated behind your filtered networks.

~ Export the tables using the `Export Data as Excel` option.

~ Conduct a neighborhood analysis for a node of interest using the different levels under `Connections`.

Sources Cited

Apicella, Coren L., Frank W. Marlowe, James H. Fowler, and Nicholas A. Christakis. 2012. "Social Networks and Cooperation in Hunter-Gatherers." *Nature* 481(7382):497-501.

Bott, Elizabeth. 1957. *Family and Social Network: Roles, Norms, and External Relationships in Ordinary Urban Families*. London: Tavistock Publications Limited.

Bright, David A., Caitlin E. Hughes, and Jenny Chalmers. 2012. "Illuminating Dark Networks: A Social Network Analysis of an Australian Drug Trafficking Syndicate." *Crime, Law & Social Change* 57(2):151-76.

Christakis, Nicholas A., and James H. Fowler. 2009. *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives*. New York: Little, Brown and Company.

Croft, Darren P., Richard James, and Jens Krause. 2008. *Exploring Animal Social Networks*. Princeton, NJ: Princeton University Press.

DellaPosta, Daniel. Forthcoming. "Network Closure and Integration in the Mid-20th Century American Mafia." *Social Networks*.

Green, Ben, Thibaut Horel, and Andrew V. Papachristos. 2017. "Modeling Contagion through Social Networks to Explain and Predict Gunshot Violence in Chicago, 2006 to 2014." *Journal of American Medical Association Internal Medicine* 177(3):326-33.

Haynie, Dana L. 2001. "Delinquent Peers Revisited: Does Network Structure Matter?" *American Journal of Sociology* 106(4):1013-57.

Kadushin, Charles. 2012. *Understanding Social Networks: Theories, Concepts, and Findings*. New York: Oxford University Press.

Krebs, Valdis E. 2002. "Mapping Networks of Terrorist Cells." *Connections* 24(3):43-52.

Malm, Aili E., and Gisela Bichler. 2011. "Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets." *Journal of Research in Crime and Delinquency* 48(2):271-97.

Mastrobuoni, Giovanni, and Eleonora Patacchini. 2012. "Organized Crime Networks: An Application of Network Analysis Techniques to the American Mafia." *Review of Network Economics* 11(3):1-41.

McClurg, Scott D. 2003. "Social Networks and Political Participation: The role of Social Interaction in Explaining Political Participation." *Political Research Quarterly* 56(4):449-64.

McGloin, Jean Marie. 2005. "Policy and Intervention Considerations of a Network Analysis of Street Gangs." *Criminology & Public Policy* 4(3):607-36.

Martina, Morris, and Mirjam Kretzschmar. 1997. "Concurrent Partnerships and the Spread of HIV." *AIDS* 11(5):641-8.

Morselli, Carlo. 2009. "Hells Angels in Springtime." *Trends in Organized Crime* 12(2):145-58.

Papachristos, Andrew V. 2009. "Murder by Structure: Dominance Relations and the Social Structure of Gang Homicide." *American Journal of Sociology* 115(1):74-128.

Papachristos, Andrew V., and Christopher Wildeman. 2014. "Network Exposure and Homicide Victimization in an African American Community." *American Journal of Public Health* 104(1):143-50.

Pedahzur, Ami, and Arie Perliger. 2006. "The Changing Nature of Suicide Attacks: A Social Network Perspective." *Social Forces* 84(4):1987-2008.

Schaefer, David R., Martin Bouchard, Jacob T. N. Young, and Derek A. Kreager. Forthcoming. "Friends in Locked Places: An Investigation of Prison Inmate Network Structure." *Social Networks*.

Sierra-Arevalo, Michael, and Andrew V. Papachristos. 2015. "Applying Group Audits to Problem Oriented Policing." Pp. 27-46 in *Disrupting Criminal Networks: Network Analysis in Crime Prevention*, edited by G. Bichler and A. E. Malm. Boulder, CO: Lynne Rienner Publishers, Inc.

Smith, Chris M., and Andrew V. Papachristos. 2016. "Trust Thy Crooked Neighbor: Multiplexity in Chicago Organized Crime Networks." *American Sociological Review* 81(4):644-67.

Travers, Jeffrey, and Stanley Milgram. 1969. "An Experimental Study of the Small World Problem." *Sociometry* 32(4):425-43.

Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press.

Watts, Duncan J. 2003. *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton & Company.

Watts, Duncan J., and Peter Sheridan Dodds. 2007. "Influentials, Networks, and Public Opinion Formation." *Journal of Consumer Research* 34(4):441-58.

Wimmer, Andreas, and Kevin Lewis. 2010. "Beyond and Below Racial Homophily: Erg Models of a Friendship Network Documented on Facebook." *American Journal of Sociology* 116(2):583-642.

National Network
For Safe Communities
at JOHN JAY COLLEGE

John Jay College of Criminal Justice
500 56th Street, Suite 031W
New York, NY 10019
Tel: (646) 557 4760
Email: info@nnscommunities.org