1 Chapter 10: Tools

1.1 HIVE

We use Hive to manage our list of incidents, and links from them to the other objects and data connected to incident responses. Check https://hive.thlab.ninja/index.html#!/cases and search for the incident name. All incidents will have the tag "disinformation" and word "Incident" in the title, which should help with searching.

1.1.1 (Adding an object workflow to a Hive Incident - don't use this yet)

Adding a new workflow to a case:
1. Assume the current Case ID is (A).
2. Create a new Case (B) selecting the workflow Case Template you wish to add to Case (A).
3. Open Case (A) and click "merge".
4. Select "By Number" and add Case ID (B).

1.2 MISP

Our main MISP instance is **https://covid-19.iglocska.eu** - we share this with the whole of the CTI League.

https://bbb.secin.lu/b/ale-q6v-ecn <-- Recorded MISP Training for COVID courtesy the CIRCL folks

1.2.1 Adding an object (tweet etc) to MISP by hand

- Go to MISP **https://covid-19.iglocska.eu**
    - Click on the incident ID in the list of events.
- Click on “Add Object” in the left-side column
    - Misc -> microblog for twitter or Facebook posts
    - Fill out the details
    - Click submit
    - Repeat for more objects
- Now you can start playing with the grey bar at the bottom of the event description, and toggle things like the timeline on and off.

Object types we’re most likely to need are:

Object	**Misp**	**Hive equivalent**
Facebook group	misc:facebook-group	url
Facebook page	misc:facebook-page	url
Facebook account	misc:facebook-account	url
Facebook post	misc:facebook-post	url
Twitter account	misc:twitter-account	url
Twitter list	misc:twitter-list	url
Twitter post	misc:twitter-post (was misc:microblog)	url
Blogsite	network:url	url
Blog account	misc:user-account	url
Blogpost	misc:blog	url
Reddit group (subreddit)	misc:reddit-subreddit	url
Reddit account	misc:reddit-account	url
Reddit post	misc:reddit-post	url
Reddit post comment	misc:reddit-comment	url
YouTube Channel	misc:youtube-channel	url

YouTube Video	misc:youtube-video	url
YouTube Playlist	misc:youtube-playlist	url
YouTube Comment	misc:youtube-comment	url
Website address	network:url	url
Hashtag	ADD NEW	hashtag
Instant message	misc:instant-message	
Instant message group	misc:instant-message-group	
Narrative	misc:narrative	
Image	file:image	
Meme	file:meme-image	
Individual	misc:person	
Event (e.g. protest)	misc:scheduled-event	
Location	misc:geolocation	

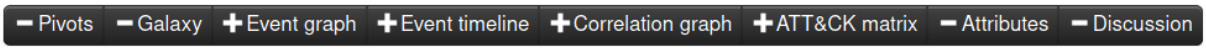
Other objects we might need include:

Object	**Misp**	**Hive equivalent**
	misc:course-of-action	
	network:email	
	file:forged-document	
	file:leaked-document	
	misc:legal-entity	
	misc:news-agency	
	misc:organization	
	misc:scheduled-event	
	misc:short-message-service	

	network:shortened-link	
	misc:user-account	

1.2.2 Adding an object to MISP via Slack bot

- Slack bots can quickly create and append an object to an event.
- Each bot attempts to modify the MISP event directly. If it lacks permission it will instead create a MISP event extension. Click the icon shown below to switch to extended mode to see the extended event objects appended into the main event.

- 

1.2.2.1 Twitter Posts

There's a Slackbot in #4-disinformation that can upload a Twitter post to a MISP event. The bot works like this /misp_twitter $MISP_event_id $post_id
It accepts either a Twitter Status ID or a Twitter post URL as arguments for $post_id

- In the #disinformation channel use the following command to add a Twitter post to the CTI League MISP
  - /misp_twitter <misp event id> <twitter post URL or twitter post ID>
  - Example: /misp_twitter 34 https://twitter.com/NASA/status/1259960728951365633?s=20

1.2.2.2 BuiltWith Tags

- In the #disinformation channel use the following command to add a Twitter post to the CTI League MISP
  - /misp_builtwith <misp event id> <url or domain name>
  - Example: /misp_builtwith 34 newyorkcityguns.com

1.3 DKAN

DKAN is a data warehouse tool - it's where we store large datasets and their descriptions,for analysts to use.

1.4 Gephi

1.4.1 Viewing networks with Gephi

This is a manual process with instructions created from Andy Patel's video at https://www.youtube.com/watch?time_continue=17&v=AqlT0khVuZA

- Get Gephi from https://gephi.org/users/download/ - install it.
- Start Gephi.
- Click on top menu>file>"import spreadsheet". Grab User_user_graph.csv - use all defaults
- Top menu: Go to data laboratory, "copy data to another column", click 'id', click okay.
- Go to overview. RHS: Run modularity algorithm, using defaults
- RHS: Run average weighted degree algorithm
- LHS: Click color icon, then partition, modularity class. Open palette, generate, unclick "limit number of colors", preset=intense, generate, okay
- LHS: Select "tt", ranking, weighted degree, set minsize=0.2, choose 3rd spline, apply
- LHS: Layout: OpenOrd, run. Then forceatlas2, run. Try stronger gravity, and scaling=200
- Top menu: Preview - select "black background", click "refresh". Click "Reset zoom"

Gephi has an API - these tasks could be automated.

1.5 Slack bots

We use slack bots to push artefacts to MISP.

we can now add the following object to a MISP event using the following slash commands
/misp_reddit_account
/misp_reddit_post
/misp_reddit_comment
/misp_reddit_subreddit

If we want new ones - we can build them, and [Name Redacted] wrote a handy how-to guide: https://vvx7.io/posts/2020/05/misp-slack-bot/

If we want new MISP object types, here's how to do that too:

1. Create the new object folder
    a. Git clone https://github.com/MISP/misp-objects
    b. Go into repo folder objects. It contains a subfolder for every misp object type
    c. Copy one of the existing object folders; rename the copy to the new object you want
    d. Go into the new object's folder. You'll find one file in here: definition.json. Open it for editing

2. Set basic data
    a. Get a new UUID from https://www.uuidgenerator.net/ - replace “uuid” in definition.json with this new one
    b. Set “version” to 1
    c. Set “name” to the same as the new folder name (nb use “-” not “_”)
    d. Set “description” to something descriptive
    e. “Meta-category” is usually “misc”
3. Set attributes. Go through attributes. For each one, set:
    a. “Description”: something descriptive
    b. “Misp-attribute”: see https://www.circl.lu/doc/misp/categories-and-types/. You’ll probably use “text” a lot. The difference between url and link? url isn’t trusted; link is trusted (this signals whether something is safe to click on).
    c. “Ui-priority”: just leave this as default (1 is always okay)
4. These attributes aren’t mandatory, but are useful
    a. “Multiple”: set this to “true” if you allow multiple of this attribute (e.g. hashtags)
    b. "disable_correlation": true, - stops MISP trying to correlate this attribute - set this on things like language to stop MISP from wasting time
    c. "to_ids" - makes exportable via api - set to false as needed (most attributes don’t need it)
5. Set the list of attributes that an object must have one of to exist
    a. List these in “requiredOneOf”
6. Check the new object is valid
    a. Run validate_all.sh
    b. Run jq_all_the_things.sh
7. Push your change back to the MISP objects repo (or to [Name Redacted] for sanity-checking)

1.6 Python scripts

We use python a lot (just look at the github repo…). Here are some useful resources:

- Learn python the hard way
- ACTION: [Name Redacted] add notes on python and data science - [Name Redacted] - level friendly

1.7 Other Tools

We’ve mentioned a bunch of tools above.

Some basic tools:

- Most data scientists use Python and Jupyter notebooks. You’ll see a lot of these - the basic Anaconda install comes with most of the things we use https://www.anaconda.com/distribution/
- Data gathering:

    - Reaper https://github.com/ScriptSmith/reaper https://github.com/ScriptSmith/socialreaper https://reaper.social/ - scrapes Facebook, Twitter, Reddit, Youtube, Pinterest, Tumblr APIs
- Network analysis and visualisation: there are many tools for this.
    - Gephi is a good standalone tool https://gephi.org/users/install/
    - Networkx is a useful python library
- URL analysis
    - Builtwith.com
- Image analysis
    - Reverse image search: tineye.com, Bellingcat guide
    - Image search: bing.com, yandex.com
    - Image text extraction: bing.com, yandex.com
- Data storage / Threat Intelligence tools
    - DKAN https://getdkan.org/
    - MISP https://www.misp-project.org/

Disinformation-specific tools:

- Indiana University has a set of tools at https://osome.iuni.iu.edu/tools/
    - Botometer: check bot score for a twitter account and friends https://botometer.iuni.iu.edu/#!/
    - Hoaxy: check rumour spread (uses Gephi) https://botometer.iuni.iu.edu/#!/
    - Botslayer https://osome.iuni.iu.edu/tools/botslayer/
- Bellingcat made a list of useful tools
    - Bellingcat's really big tools list - worth reading if you need a specific OSINT tool