

# OSINT for Pen Tests

No Subtitle Yet; Open to Suggestions

# About Me

- Emily
- Sol (@g\_solaria on twitter)
- OSINT consultant, often for private clients and small/medium businesses.

# About this talk:

- Going to cover OSINT workflow and how it can be used in pen tests.
- Not covering specific tools in depth, but will point out which tools can be used in specific situations.
- Tools will be linked in notes on GitHub, along with tutorials I've found useful.

# What is OSINT?

- OSINT = Open Source INTelligence
- This is information that can be gained from public sources
- Includes things like paper court records and old publications
- For our purpose we're focusing on Internet-based OSINT.

# How can OSINT be used during pen tests?

- Used during the recon stage
- Used to find infrastructure, technologies, and employee information

# Workflow

- OSINT workflow:
  - Once you're given a target, determine the best place to start.
    - Employees? Infra? Technology?
    - This will be determined by a lot of things including the scope, time restraints, etc.

# Workflow (con't)

- What information are you looking for about this thing?
  - Infra: domains, cloud, internet-facing servers
  - Technologies: Apps deployed on network, web based apps , etc.
  - Employees: Personal social media/online accounts, schedules, org chart, emails, etc.

# Repeat Your Steps

- Every time you find a new piece of information, run it through the same process.
  - You may find that pieces of information start to spider out off of other information.



# Infrastructure

- As with the over-all workflow, where you start with infrastructure depends on scope and time restrictions.
  - Figure out a list of domains.

# Infrastructure (Con't)

- Run this list through various tools such as PassiveTotal or Maltego to get sub domains.
  - Sub domains may expose applications that are in use
  - All of this can be done from within Maltego using the PassiveTotal API, and the transforms available for Maltego.
    - Allows for greater visualization.
- Use a tool like recon-ng's cert transparency module to discover even more sub-domains.
  - Sometimes turns up sub-domains that aren't listed by PassiveTotal.

Resolutions 1680

WHOIS 4

Subdomains 148

Trackers 1000

Components 1000

Host Pairs 2000

Hashes 816

DNS 16

Cookies 1000

## FILTERS ⓘ

## HOSTNAME (148 / 148)

- ✓ ✕ access.bestbuy.... 1
- ✓ ✕ accesspl.bestbu... 1
- ✓ ✕ advertising.best... 1
- ✓ ✕ airwatch.bestb... 1
- ✓ ✕ api-stage.bestb... 1

[Show More...](#)

## TAG

## SYSTEM TAG (2 / 149)

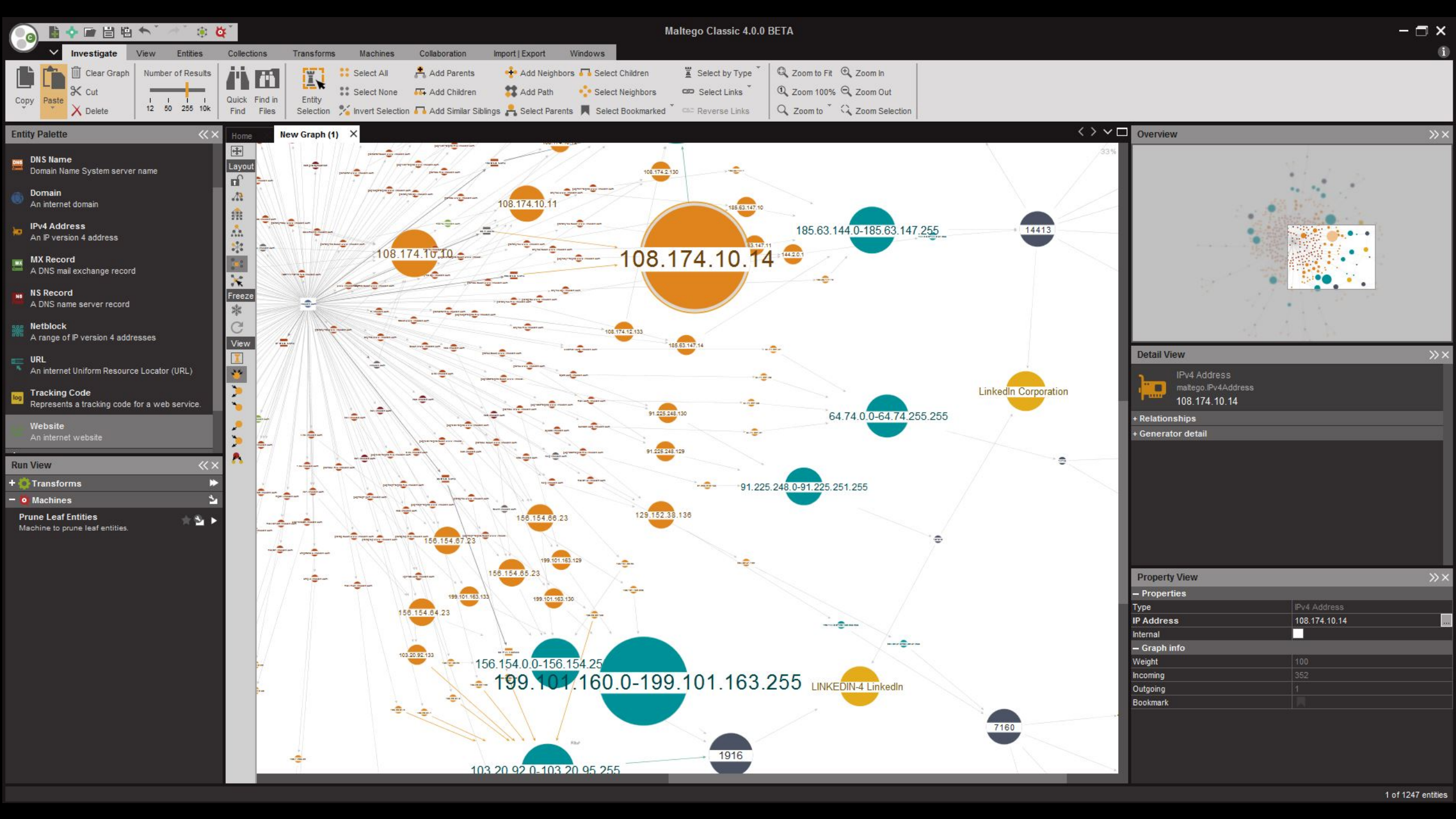
- ✓ ✕ registered 148
- ✓ ✕ known\_compro... 1

## SUBDOMAINS ⓘ

☐ ▼ Show : 25 1-25 of 148 ▶ Sort : Hostname Ascending ▼[Download](#) [Copy](#)

Hostname	Tags
<input type="checkbox"/> <a href="#">access.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">accesspl.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">advertising.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">airwatch.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api-stage.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api-status.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api-test.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api.bbyremix.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api.bestbuy.com</a>	<a href="#">Registered</a>
<input type="checkbox"/> <a href="#">api.deals.bestbuy.com</a>	<a href="#">Registered</a>





## Entity Palette



### DNS Name

Domain Name System server name



### Domain

An internet domain



### IPv4 Address

An IP version 4 address



### MX Record

A DNS mail exchange record



### NS Record

A DNS name server record



### Netblock

A range of IP version 4 addresses



### URL

An internet Uniform Resource Locator (URL)



### Tracking Code

Represents a tracking code for a web service.



### Website

An internet website

# Infrastructure (Con't)

- Look at trackers on the domains you're researching.
  - GoogleAnalytics, AdSense IDs, etc., can reveal additional domains.
  - PassiveTotal and Maltego can both accomplish this.



[www.forums.bestbuy.com](http://www.forums.bestbuy.com)

2015-11-18

2017-10-12

GoogleAnalyticsAccountNumber

[ua-27719495](#)

 Registered



[investors.bestbuy.com](http://investors.bestbuy.com)

2015-09-29

2017-10-12

GoogleAnalyticsAccountNumber

[ua-55691474](#)

 Registered

# Infrastructure (Con't)

- Use tools like DNS Map to brute additional sub domains.
  - DNS Map can be provided with a wordlist. Use this to look for common apps that may be hosted on their own sub domain.
- List out your subdomains and any corresponding information
  - IP addresses
  - Hosting (is it internally hosted, cloud-based, etc?)

# Repeat Every Step, Every Time

Each time you pull up a new piece of information, run it through your tools again to see if it will point you to even more new info.



# Technologies

- Ask the same questions – What are you looking for, and where is the best place to start?
  - Applications and services on the network, web apps that they may be using, etc.
- What's the scope of the pen test?
  - Is there anything you're not supposed to touch?

# Technology

- Use tools like Shodan.io to begin looking at individual IPs gathered during the infrastructure recon.
  - Often pulls banners of services running.
  - May have screenshots of things like RDP that reveal credentials without the need to hit that IP yourself.

# Technology (Con't)

- Various other open source tools such as nmap.
- Maltego and Recon-ng will also have transforms and modules for this.

# Technologies

- Look for a company GitHub.
  - Additionally look for employees that are using public github repos to store work-related things.
- Use or develop tools to scrape sites like Pastebin for pastes with relevant keywords.

Once Again:

Each time you pull up a new piece of information, run it through your tools again to see if it will point you to even more new info.

# Why target employees?

- People are incompetent.
- They may leak information about the organization.
- Less work if you need to resort to social engineering.
- Gives you an idea of who in the organization to target for these attempts.
- The laughs.



Hack Corp  
Beta version

Original Developers  
Laz and Nitrous

# Employees

- Who are your target employees?
  - Look for people in IT/InfoSec
  - Also look for HR, sales, and other non-technical employees. These employees may still leak relevant information.
- What information do you have about these employees?
  - If none this is your starting point.
  - If you have a list of names, begin with real name searches.



# Employees (Con't)

- What information do you have about these employees?
  - If none this is your starting point.
  - If you have a list of names, begin with real name searches.

# Finding Employees

- General searches:
  - Do they have employee staff pages?
  - Have any of their employees given talks, done interviews, etc.
  - Do they highlight employees on their social media at all?
- Tools:
  - LinkedIn
    - LinkedIn in general has a ton techniques for getting lists of employees.
    - LinkedIn takes this to the next level and integrates all of these into one tool
  - Facebook searches
    - People often put their employers on their Facebook profile, which is searchable using the search URLs.

# LinkedIn and LinkedInt

- LinkedIn:
  - Company pages will often list employee accounts, but information will be redacted.
    - Manual workarounds include
      - Doing an exact search for their title on Google (site:linkedin.com “exact title here”)
      - Looking through the connections of the “people also viewed” section
      - Reverse image searching the profile image.
- LinkedInt:
  - Allows for scraping email addresses from LinkedIn with minimal effort

# Real Name searches

- Begin looking at individual employees that you'd like to target.
  - This can also lead you to other employees who may be even better targets.
  - As with the people/infra/tech decision, rank by who is most valuable, and also most likely to provide good info.
    - A sysadmin with minimal footprint online may be a less valuable target than an HR manager who is constantly posting on Facebook.
- Things you want to determine first:
  - Work email address(es)
  - Social Media accounts
  - Personal email addresses.
  - Account usernames.

# Tools for Real Name Searches

- There are a number of free and paid tools, each of which has different strengths/weaknesses.
  - Pipl, That's Them, etc. (free)
  - Spokeo (paid)
- As you find pieces of info, run them through multiple tools to turn up new information.
  - Do this process with each new piece of info you find.
  - New pieces of info may pull up different results with even more new info.
  - For instance, if you get a phone number from That's Them, search the phone number on That's Them and Pipl as well.

# Username

- Employee usernames are valuable even if they're not work-related
  - Can be used to find discussions between employees.
  - Employees asking work-related questions on support forums
    - (Monitor things like Twitter, StackExchange, etc., for the duration of pen test. May give hints about technologies being used/configurations.)
    - Performing continuous monitoring using Google Alerts, or even scripts that use the Google CSE API will allow you to catch things that may be deleted.
  - Look for employee GitHub accounts, or GitHub accounts belonging to the company.
  - Tools like Namechk.com can be used to find additional accounts.
  - Don't neglect search engines and search operators.

# Emails

- Both personal and corporate emails can be useful.
  - Employees often check personal emails from work computers.
- Various tools exist that will allow you to generate and check email addresses.
  - Incredibly easy to script your own if you don't want to leave a footprint on someone else's server

# Social media

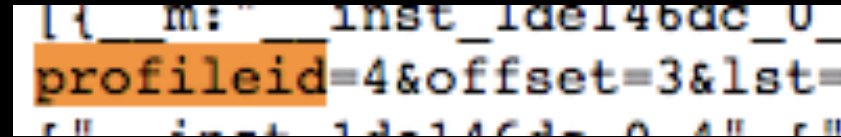
- Employees may post photos of work environment.
- Post about various technologies they use.
- Allow for greater intel collection on potential SE targets.
- Give ideas of what their schedule is like, when people are in the office.
- In general people talk too much on social media. You will find useful info.
- Most social media sites have better search methods than the search bar.



# Facebook

- Many people put their employers on Facebook.
  - This information is searchable.
  - You can search by employer or search for people employed by the same company as your target.
- Search URLs:
  - Use them, they're better than the form.
  - Get profileID (right click on profile, search on page for profileID)
  - URL format to find employees of a company:
    - <https://www.facebook.com/search/str/<companypageID>/employees>

# Facebook URL LIST



l\_t\_m: inst\_idel46dc\_0\_  
profileid=4&offset=3&lst=  
f" inst\_1de146dc\_0\_4" f"

- <https://www.facebook.com/search/<profileID>/<searchitem>>
  - Filling in the profile ID with any number of allowed searches will pull up a list of that profile's posts/comments/etc on Facebook
- <https://www.facebook.com/search/<profileID>/friends/<searchitem>>
  - Presents you with a list of the same, but for the target's friends.
- <https://www.facebook.com/search/<profileIDx>/searchitem/<profileIDy>/searchitem/intersect>
  - Shows where two people have interacted with the same posts/comments/etc.

# Available Search Options

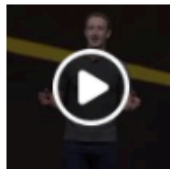
places-visited	videos	events-joined
recent-places-visited	videos-by	stories-by
places-checked-in	videos-of	stories-commented
pages-liked	videos-liked	stories-tagged
photos-by	videos-commented	groups
photos-liked	apps-used	employees
photos-of	friends	relatives
photos-commented	events	



**Mark Zuckerberg** ✓

October 11 at 2:42pm · 🌐

Here's my keynote at Oculus Connect.



👍❤️👤 104K

6.4K Comments 9.3K Shares



**Mark Zuckerberg** ✓ is at 📍 **Oculus Connect 4.**

October 11 at 10:33am · San Jose, CA · 🌐

Today we announced Oculus Go -- the most accessible virtual reality experience we've ever built. Oculus Go is a standalone headset that doesn't require you to snap in a phone or attach a cable. It's great for playing games, watching movies,...[See more](#)



👍❤️👤 90K

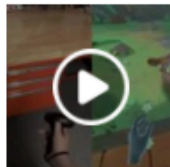
4.6K Comments 5.3K Shares



**Mark Zuckerberg** ✓ shared **Oculus's live video.**

October 11 at 10:03am · 🌐

Live at Oculus Connect talking about the future of VR.



👍❤️👤 Muna Thapa Magar, Boz and 36K others

930 Comments 3 Shares



**Mark Zuckerberg** ✓

October 10 at 3:30pm · Menlo Park, CA · 🌐

I'm thinking of everyone affected by the wildfires in California. In the

1

**Los Angeles, California**

[Learn More](#)

👍 Liked

2

**Moscow, Russia**

[Learn More](#)

👍 Like

3

**Panama City, Panama**

[Learn More](#)

👍 Like

4

**Abuja, Nigeria**

👍 Like

5

**The Walmart Museum**

4.4 ★★★★★ (550) · Museum · \$\$\$\$

105 N Main St · (479) 273-1329 · [Open Now](#)

[Contact Us](#)

👍 Like



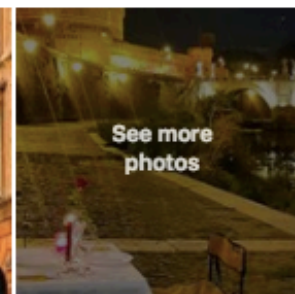
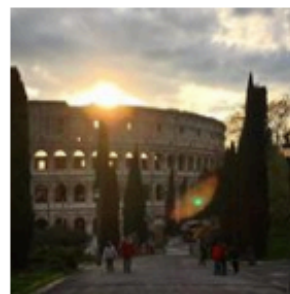
Very informative about the history, without feeling like they were pushing the brand on us, or advertising. "

Glen Goering · 4.0 ★ · over a year ago

6

**Singapore**

👍 Like



[See more photos](#)

# Organization of OSINT

- Set a standard for organizing your findings.
  - Maltego has tools built in for this.
  - Make sure each piece of information you gather is put somewhere so you don't have to go looking for it.
  - Things can change quickly, so screenshot everything, the first time. Don't count on it being there for you to go back to later.

# Tools You Should Know

- Recon-ng
  - Metasploit for the OSINT.
  - Allows you to add API keys to make use of third party services.
  - Modules can be written in Python
- Maltego
  - Allows visualization of infrastructure and people.
  - Uses transforms that run on “seeds.” (Community edition)
  - Allows you to make use of third party services using API keys.
- DNS Map
  - Brutes subdomains.

OSINT Can be Noisy

Test everything first!

- Make sure the various methods you're using aren't going to be noticeable.
  - Create social media accounts and test various methods to see if they leave footprints.
  - Get to know what the logs from your tools will look like. Check this often.



Questions?