OSINT: Open Source Intelligence

Josh Huff | All Rights Reserved
Josh Huff, @Baywolf88
https://www.learnallthethings.net

- Digital Forensics Analyst
- Private Investigator
- Information Security Conference Speaker
- ColaSec Meetup Co-organizer
- Blogger
OSINT defined:

Intelligence from publicly available information that is collected exploited, and reported to address a specific intelligence requirement.
What is OSINT?

OSINT is Open Source INTelligence
Information in the public domain or accessible from public sources

- Media such as audio, video and pictures
- Text from documents, articles and blogs
- Maps and geolocation of data

Social Media
- Sometimes called SOCMINT for SOCial Media INTelligence
Who uses OSINT?

What professions can leverage OSINT data?

• Information Security
• Private Investigators
• Law Enforcement
• Businesses
• Attorneys

Who Else?
Who else uses OSINT?

What else uses OSINT data?
- Vacation planning
- Car Buying
- Baby Sitter Selection
- Online Dating
- House Hunting

Who Else? Everybody uses OSINT
How do we Collect OSINT?

Collecting OSINT

Tools and Resources
(The Fun part)

2 Personal Favorites:
OSINT Framework
IntelTechniques
Resources – OSINTFramework by Justin Nordine

OSINT Framework

www.osintframework.com
Resources – IntelTechniques by Michael Bazzell

https://inteltechniques.com/menu.html
300+ page handbook of tools
https://start.me/p/m6XQo8/osint
(Technisette Start Page of Tools and Tutorials)
https://start.me/p/VRxaj5/dating-apps-and-sites-for-investigators
(Emmanuelle Welch OSINT on Dating sites)
https://start.me/p/ZME8nR/osint
(Bruno Mortier collection of Search sites)
https://start.me/p/W2kwBd/sources-cnty
(Bruno Mortier OSINT by Country)
https://start.me/p/ZME8nR/osint
(Bruno Mortier Collections of Collections)
Use Case – Identifying a vehicle
Enhance the Image

For a closer look
Hunting for a tail light
After Searching

Jeep Liberty Sport VS Dodge Durango
Data Validation with Berla
# Data Validation with Berla

## 2005 Jeep Liberty Sport

<table>
<thead>
<tr>
<th>Basic Data</th>
<th>Engines</th>
<th>Transmissions</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wheelbase</td>
<td>104.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross Vehicle Weight Range</td>
<td>4000-5000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seating</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Seating</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>174.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fuel Tank 1 Capacity (Gallons):** 20

## 2004 Dodge Durango SLT

<table>
<thead>
<tr>
<th>Basic Data</th>
<th>Engines</th>
<th>Transmissions</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wheelbase</td>
<td>119.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross Vehicle Weight Range</td>
<td>6001-7000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seating</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Seating</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>200.8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fuel Tank 1 Capacity (Gallons):** 27
Data Validation with Berla

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wheelbase</td>
<td>119.2</td>
</tr>
<tr>
<td>Gross Vehicle Weight Range</td>
<td>6001-7000</td>
</tr>
<tr>
<td>Seating</td>
<td>7</td>
</tr>
<tr>
<td>Max Seating</td>
<td>7</td>
</tr>
<tr>
<td>Length</td>
<td>200.8</td>
</tr>
<tr>
<td>Fuel Tank 1 Capacity</td>
<td>27 (Gallons)</td>
</tr>
</tbody>
</table>
Preserve OSINT Research

Screenshots

Full Browser Capture
How You Work Impacts End Results

Creepy Google Person  Vs  Professional
The OSINT Cycle

Requirements gathering

Retrieving data

Analyzing information

Pivoting to a new perspective or Reporting analysis
SEC487: Open-Source Intelligence Gathering (OSINT) and Analysis

https://www.sans.org/sec487

- 6 days, 36 CPEs
- Over 20 hands-on labs
- Geared towards everyone: beginner to expert
What do we do to protect ourselves?

OSINT yourself

What common identifiers of YOU are online right now?
Did you find a lot?

Opt-Outs

Share this awareness with:
Co-workers and Family Members

webbreacher.com/2017/04/24/removing-yourself-from-the-internet
Conclusions

OSINT is for Everyone

MANY free OSINT tools online

Organization/Execution is key

Awareness = Defense

Questions?

Josh@Learnallthething.net

@baywolf88