HUNTING TOOLS

This document contains my recommendations for tools that might be helpful in your hunting process. I've mostly focused on free and open source tools for the sake of accessibility, but I've also highlighted some of my favorite commercial tools. In the cases where I've recommended commercial tools, I am not compensated for doing so. I recommend the tools I like and use myself.

SECTION 1: LOG AGGREGATION

Much of the work you'll do hunting involves performing data transformation on log data. You must have a tool that allows you to centrally aggregate those logs and interact with them. This is a basic necessity for hunting.

Recommended:

- **ELK** (https://www.elastic.co/): Free complete logging pipeline with analysis tools. Robust plugin ecosystem. Paid commercial support is available. Administration is complex at certain levels. You'll spend some on humans and infrastructure to support ELK that you are not spending on software licensing.
- **Splunk** (https://www.splunk.com/): Commercial best of breed. Free for testing and development. Billed by ingestion volume and gets very pricey at higher levels.
- **Graylog** (https://www.graylog.org/): Another Elastic-based platform. The provide a free open source version, and a commercial version.

SECTION 2: DATA MANIPULATION TOOLS

Many of the best data manipulation tools are free on the command line, or application you might traditionally use for other purposes. Scripting languages and specific libraries are also useful for this purpose.

Recommended:

- **Microsoft Excel**: This sounds silly, but it's the most robust graphical data manipulation tool that exists. Not feasible at large scale, but useful for some tasks.
- **Python** (https://www.python.org/): The scripting language of choice for most analysts. You don't have to be an expert programmer to be a hunter, but it will help where command line tools don't meet your needs.
- **Pandas** (https://pandas.pydata.org/): A Python data analysis library used for data manipulation and statistics. You can use this to perform many of the statistical techniques discussed in the course.
- **R** (https://www.r-project.org/about.html)**:** A programming language designed for computer statistics. Very popular amongst researchers and useful for statistics described in this course.
- **Cyber Chef** (https://github.com/gchq/CyberChef): Purpose-built security tool for encoding/decoding data and general string manipulation.
- **Regex Buddy** (https://www.regexbuddy.com/): Commercial regular expression development tool. This really helps parse complex regex that you'll use for searching.

Most used Linux command line tools:

- **SED**: Stream editor for manipulating text for manipulating data and normalization.
- **AWK**: Scripting language used for manipulating and normalizing data.
- **CUT**: Used for parsing fields out of delimited data.
- **SORT**: Used for sorting data based on its properties.
- **UNIQ**: Used for identifying unique values and eliminating duplicates.
- **GREP**: Used for searching for strings within data.
- **JQ**: JSON data manipulation and parson.

HUNTING TOOLS

SECTION 3: SPECIALIZED ANALYSIS TOOLS

A significant portion of the hunter's tool kit is dedicated to analysis tools that are unique to specific data types. I've highlighted some of my favorites for many of my preferred data types here.

Realm	Type	Tool
Network	Packet Data	▪ **Wireshark/TShark** (https://www.wireshark.org/): The industry standard for packet analysis. ▪ **Moloch** (https://molo.ch/): A web-based packet indexing and analysis tool.
	Flow Data	▪ **SiLK** (https://tools.netsa.cert.org/silk/): Flow data collection with a robust set of analysis and stats tools.
Disk	File Identification	▪ **YARA** (https://virustotal.github.io/yara/): Host-based file scanning tool with shareable configurations. ▪ **Strelka** (https://github.com/target/strelka): Real-time file scanning from Target, based on LAIKA.
	General OS Inquiry	▪ **Osquery** (https://osquery.io/): Query host information like a database using SQL. ▪ **Kolide Fleet** (https://kolide.com/fleet): Web-based GUI for Osquery analysis and management. ▪ **GRR** (https://github.com/google/grr): Google's endpoint inquiry agent and console.
Memory	Memory Dumps	▪ **Volatility** (https://www.volatilityfoundation.org/): Collection of tools and framework for analyzing memory.
Friendly Intel	System Inventory	▪ **Microsoft SCCM** (https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager): Microsoft's management tool provides useful inventory reporting for hunters. ▪ **ManageEngine Asset Explorer** (https://www.manageengine.com): This space is lacking, but this tool does a decent job.

HUNTING TOOLS

Threat Intel	Reputation	▪ IP Void / URL Void (http://www.ipvoid.com/): Simple free IP and domain reputation with a reasonable data inputs. ▪ VirusTotal (https://www.virustotal.com): Google's service providing file reputation history. Massive user base. Free and commercial access.
	Ownership	▪ **Domain Tools** (https://www.domaintools.com/): Quick gateway into domain registrar and IP registry databases. Commercial service provides WHOIS history.
	Passive DNS	▪ **Passive Total** (https://community.riskiq.com/): Fantastic visuals. Unfortunately limited to a small number of queries per day unless you purchase a license. ▪ **Alienvault OTX** (https://otx.alienvault.com/): Completely free but smaller data set and clunkier interface than Passive Total.
	Sandbox	▪ **Any.run** (https://any.run/): Newer web-based tool with excellent visuals. Free and commercial versions. ▪ **Cuckoo** (https://cuckoosandbox.org/): Popular open-source tool you can install on your own hardware.
	Data Mining	▪ **Maltego** (https://www.paterva.com): Generates link graphs based on pre-made or custom transforms to identify relationships between entities.
	URL Categorization	▪ **Zvelo** (https://tools.zvelo.com/): Large queryable URL categorization database.

SECTION 4: HUNTING PLATFORMS

Sometimes it's easier to get started when the tools are already installed and configured for you. There are a few pre-built platforms that exists for exactly this purpose.

Recommended:

- **Security Onion** (https://securityonion.net/): A complete network security monitoring platform that you can deploy in a few minutes. Built around Ubuntu Linux but beginning to support more platforms. Primarily network focused, but continuing to evolve into the other areas. Contains many of the tools listed here, including ELK for log aggregation. Great support community and suitable for production deployment.
- **HELK** (https://github.com/Cyb3rWard0g/HELK): A hunting platform built around ELK. Includes many of the tools listed here including data science infrastructure for advanced stats.
- **Detection Lab** (https://github.com/clong/DetectionLab): Not exclusively hunting focused, but a useful platform for spinning up multiple Windows/Linux systems at once and testing behaviors to see what they might look like. I use a similar lab setup to help develop hunting techniques and understand what normal looks like.

SECTION 5: WORKFLOW TOOLS

Case/Ticket Management:

- **Evernote** (https://evernote.com/): This is my favorite note-taking application. It will sync between systems, allows individual sections of note content to be encrypted, and provides collaboration features. There is a free and commercial version.
- **OneNote** (https://products.office.com/en-us/onenote/digital-note-taking-app): Kinda like Evernote, but specific to the Microsoft ecosystem. Provides many of the same features although I prefer Evernote.
- **TheHive** (https://thehive-project.org/): A simple security incident response platform. I like this tool because it's not overly complex and has a clear workflow. It's also expandable through plugins. You can use this to track notable hunting expeditions.
- **JIRA** (https://www.atlassian.com/software/jira): Commercial issue and project tracking tool. This gets a bad rap because so many organizations over complicate it. The large feature set can seem like bloat, but it's easy to slim it down to a place where it's great for managing your hunting workflow and interesting investigations.
- **ServiceNow** (https://www.servicenow.com/ : Many large organizations use this because its capability is limitless if you can throw enough human resources at it. It also can serve the role of help desk ticket system, which can be handy. It's very bloated, but if you have highly custom workflows and people/money/time to invest then it can really shine in the right environments.

Wiki Software:

- **Doku Wiki** (https://www.dokuwiki.org/dokuwiki): My favorite free wiki because it's incredibly simple without a lot of bells and whistles. It looks a bit antiquated, but gets the job done.
- **Confluence** (https://www.atlassian.com/software/confluence): My preferred commercial wiki. It has a lot of features while not feeling overly bloated. Made by the same company who provides JIRA, so the ability to link from workflow tickets to wiki articles comes in handy.

SOAR:

- **Komand** (https://www.komand.com/): I really like the simplicity and extendibility of this orchestration too which can help automate hunting data retrieve and transformation. The graphical workflow editor is well-designed.