



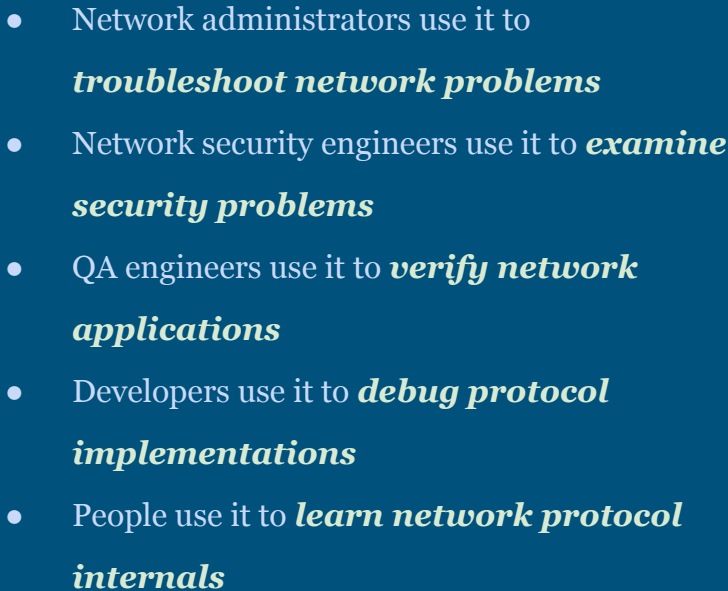
# Advanced Cyber: Network Security



Omar Salih



\_\_\_\_\_



- Network administrators use it to ***troubleshoot network problems***
- Network security engineers use it to ***examine security problems***
- QA engineers use it to ***verify network applications***
- Developers use it to ***debug protocol implementations***
- People use it to ***learn network protocol internals***

# WIRESHARK Features:

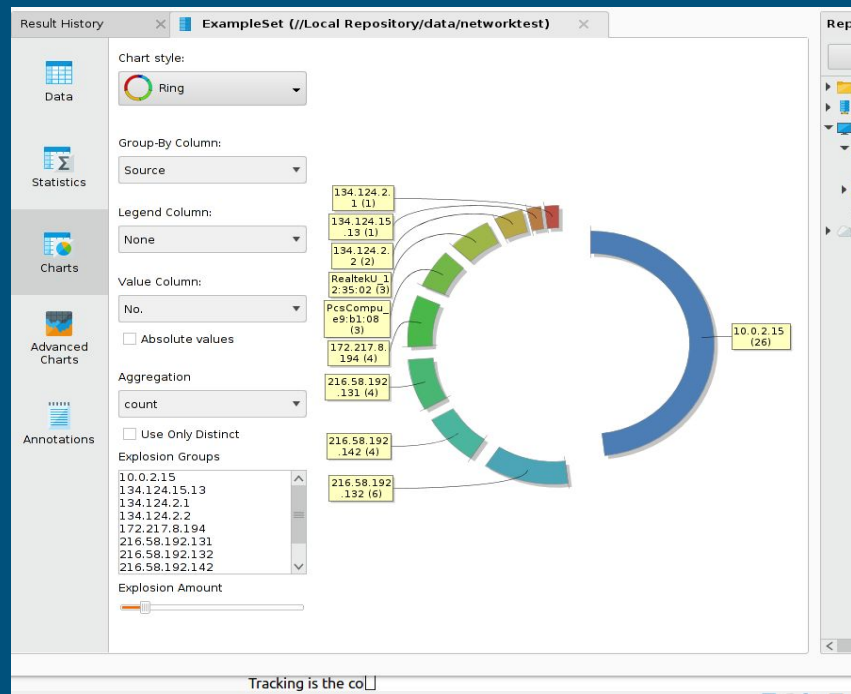
---

The following are some of the many features Wireshark provides:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• Available for <i>UNIX</i> and <i>Windows</i>.</li><li>• <i>Capture</i> live packet data from a network interface.</li><li>• <i>Open</i> files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.</li><li>• <i>Import</i> packets from text files containing hex dumps of packet data.</li></ul> | <ul style="list-style-type: none"><li>• Display packets with <i>very detailed protocol information</i>.</li><li>• <i>Save</i> packet data captured.</li><li>• <i>Export</i> some or all packets in a number of capture file formats.</li><li>• <i>Filter packets</i> on many criteria.</li><li>• <i>Search</i> for packets on many criteria.</li><li>• <i>Colorize</i> packet display based on filters.</li><li>• Create various <i>statistics</i>.</li></ul> |
|--|---|

# WIRESHARK Data: Analytics After Ran Thru RapidMiner

RapidMiner Studio is a visual workflow designer. It allows for rapid prototyping of ideas, as well as designing mission critical predictive models.



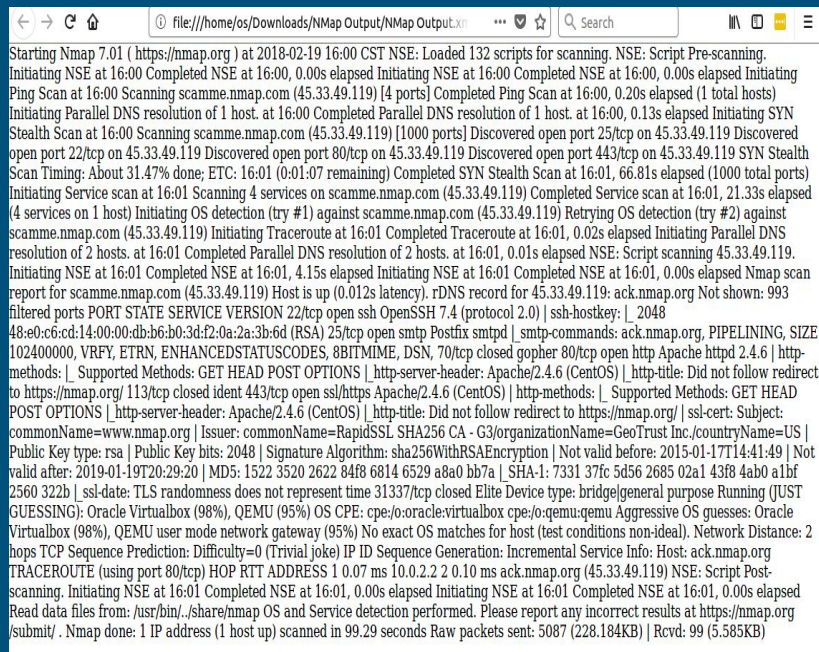
# RapidMiner Studio:

---

Streamlines transformation, development & validation of data by using:

|  |  |
|--|--|
| <b>DATA MODELING</b><br>Connect to any data source, any format, at any scale | <b>DATA CLEANSING</b><br>Expertly cleanse data for advanced algorithms   |
| <b>DATA EXPLORATION</b><br>Quickly discover patterns or data quality issues  | <b>MODELING</b><br>Efficiently build and delivers better models faster   |
| <b>DATA BLENDING</b><br>Create the optimal data set for predictive analysis  | <b>VALIDATION</b><br>Confidently & accurately estimate model performance |

# NMap



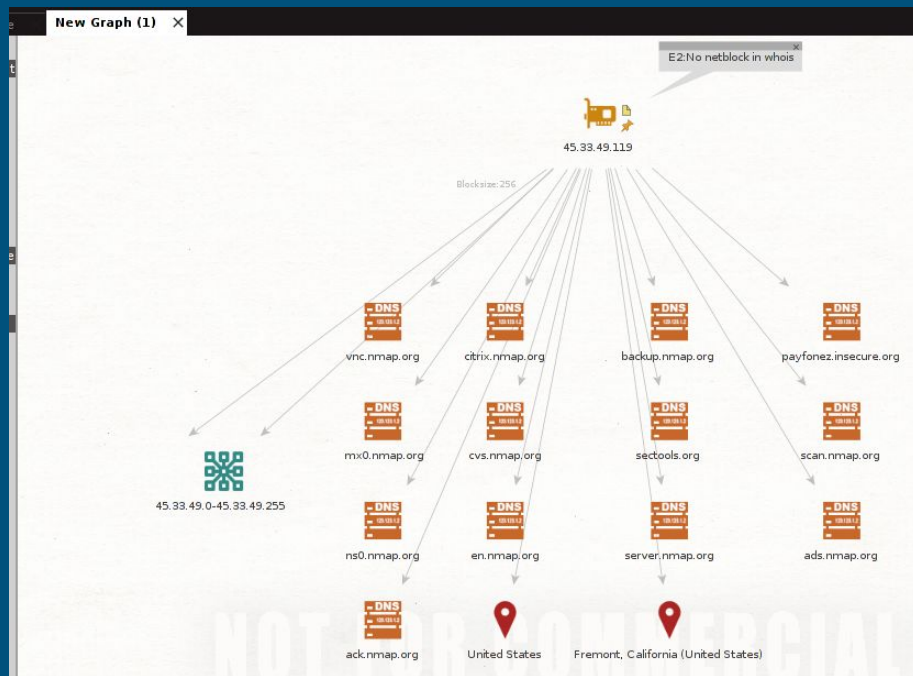
```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-02-19 16:00 CST NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning.
Initiating NSE at 16:00 Completed NSE at 16:00, 0.00s elapsed Initiating NSE at 16:00 Completed NSE at 16:00, 0.00s elapsed Initiating
Ping Scan at 16:00 Scanning scamme.nmap.com (45.33.49.119) [4 ports] Completed Ping Scan at 16:00, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:00 Completed Parallel DNS resolution of 1 host. at 16:00, 0.13s elapsed Initiating SYN
Stealth Scan at 16:00 Scanning scamme.nmap.com (45.33.49.119) [1000 ports] Discovered open port 25/tcp on 45.33.49.119 Discovered
open port 22/tcp on 45.33.49.119 Discovered open port 80/tcp on 45.33.49.119 Discovered open port 443/tcp on 45.33.49.119 SYN Stealth
Scan Timing: About 31.47% done; ETC: 16:01 (0:01:07 remaining) Completed SYN Stealth Scan at 16:01, 66.81s elapsed (1000 total ports)
Initiating Service scan at 16:01 Scanning 4 services on scamme.nmap.com (45.33.49.119) Completed Service scan at 16:01, 21.33s elapsed
(4 services on 1 host) Initiating OS detection (try #1) against scamme.nmap.com (45.33.49.119) Retrying OS detection (try #2) against
scamme.nmap.com (45.33.49.119) Initiating Traceroute at 16:01 Completed Traceroute at 16:01, 0.02s elapsed Initiating Parallel DNS
resolution of 2 hosts. at 16:01 Completed Parallel DNS resolution of 2 hosts. at 16:01, 0.01s elapsed NSE: Script scanning 45.33.49.119.
Initiating NSE at 16:01 Completed NSE at 16:01, 4.15s elapsed Initiating NSE at 16:01 Completed NSE at 16:01, 0.00s elapsed Nmap scan
report for scamme.nmap.com (45.33.49.119) Host is up (0.012s latency). rDNS record for 45.33.49.119: ack.nmap.org Not shown: 993
filtered ports PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.4 (protocol 2.0) | ssh-hostkey: | 2048
48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA) 25/tcp open smtp Postfix smtpd | smtp-commands: ack.nmap.org, PIPELINING, SIZE
102400000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN, 70/tcp closed gopher 80/tcp open http Apache httpd 2.4.6 | http-
methods: | Supported Methods: GET HEAD POST OPTIONS | http-server-header: Apache/2.4.6 (CentOS) | http-title: Did not follow redirect
to https://nmap.org/ 113/tcp closed ident 443/tcp open ssl/https Apache/2.4.6 (CentOS) | http-methods: | Supported Methods: GET HEAD
POST OPTIONS | http-server-header: Apache/2.4.6 (CentOS) | http-title: Did not follow redirect to https://nmap.org/ | ssl-cert: Subject:
commonName=www.nmap.org | Issuer: commonName=RapidSSL SHA256 CA - G3/organizationName=GeoTrust Inc./countryName=US |
Public Key type: rsa | Public Key bits: 2048 | Signature Algorithm: sha256WithRSAEncryption | Not valid before: 2015-01-17T14:41:49 | Not
valid after: 2019-01-19T20:29:20 | MD5: 1522 3520 2622 84f8 6814 6529 a8a0 bb7a | SHA-1: 7331 37fc 5d56 2685 02a1 43f8 4ab0 a1bf
2560 322b | ssl-date: TLS randomness does not represent time 31337/tcp closed Elite Device type: bridge[general purpose Running (JUST
GUESSING): Oracle Virtualbox (98%), QEMU (95%) OS CPE: cpe:/o:oracle:virtualbox cpe:/o:qemu:qemu Aggressive OS guesses: Oracle
Virtualbox (98%), QEMU user mode network gateway (95%) No exact OS matches for host (test conditions non-ideal). Network Distance: 2
hops TCP Sequence Prediction: Difficulty=0 (Trivial joke) IP ID Sequence Generation: Incremental Service Info: Host: ack.nmap.org
TRACEROUTE (using port 80/tcp) HOP RTT ADDRESS 1 0.07 ms 10.0.2.2 2 0.10 ms ack.nmap.org (45.33.49.119) NSE: Script Post-
scanning. Initiating NSE at 16:01 Completed NSE at 16:01, 0.00s elapsed Initiating NSE at 16:01 Completed NSE at 16:01, 0.00s elapsed
Read data files from: /usr/bin/, /share/nmap OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ . Nmap done: 1 IP address (1 host up) scanned in 99.29 seconds Raw packets sent: 5087 (228.184KB) | Rcvd: 99 (5.585KB)
```

Nmap is a security scanner that is an alternative to the router-based device tracking, which is used to discover hosts and services on a computer network. Nmap scans for devices that are connected to the network that's locally being scanned. By doing this, the network will be mapped out in full detail. As an alternative, ZenMap is the GUI version of NMap.

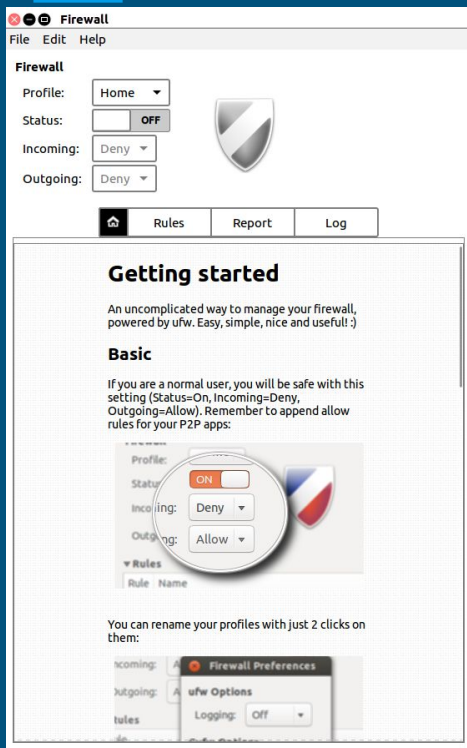
(Browser View Shown Above)

# MALTEGO

Utilized for online investigations, Maltego is a data mining tool, that is interactive, which renders graphs that is used for showing, analyzing and linking data relationships online. It clarifies how various sourced online information is related.



# FIREWALL



A firewall, or an IPTable(s) management system, are installed by default on all official Ubuntu distributions (Ubuntu, Kubuntu, Xubuntu). When an official Ubuntu distribution is installed, IPTables are there, without any traffic limitations, which allows all traffic by default. Ubuntu 8.04 LTS, introduced standard ufw firewall program that manages IPTables firewall easily. Ever since ufw was introduced as being part of Ubuntu 8.04 LTS, it has been a standard inclusion in all official linux distributions.



# References

---

Wireshark User's Guide: [https://www.wireshark.org/docs/wsug\\_html/#PreAudience](https://www.wireshark.org/docs/wsug_html/#PreAudience)

RapidMiner Studio: <https://rapidminer.com/products/studio/>

NMap: [https://home-assistant.io/components/device\\_tracker.nmap\\_tracker/](https://home-assistant.io/components/device_tracker.nmap_tracker/)

<https://en.wikipedia.org/wiki/Nmap>

Maltego CE: <https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php>

Firewall: <https://www.howtogeek.com/115116/how-to-configure-ubuntus-built-in-firewall/>

NOTE: All images are outputs, resulting from using the discussed tools.