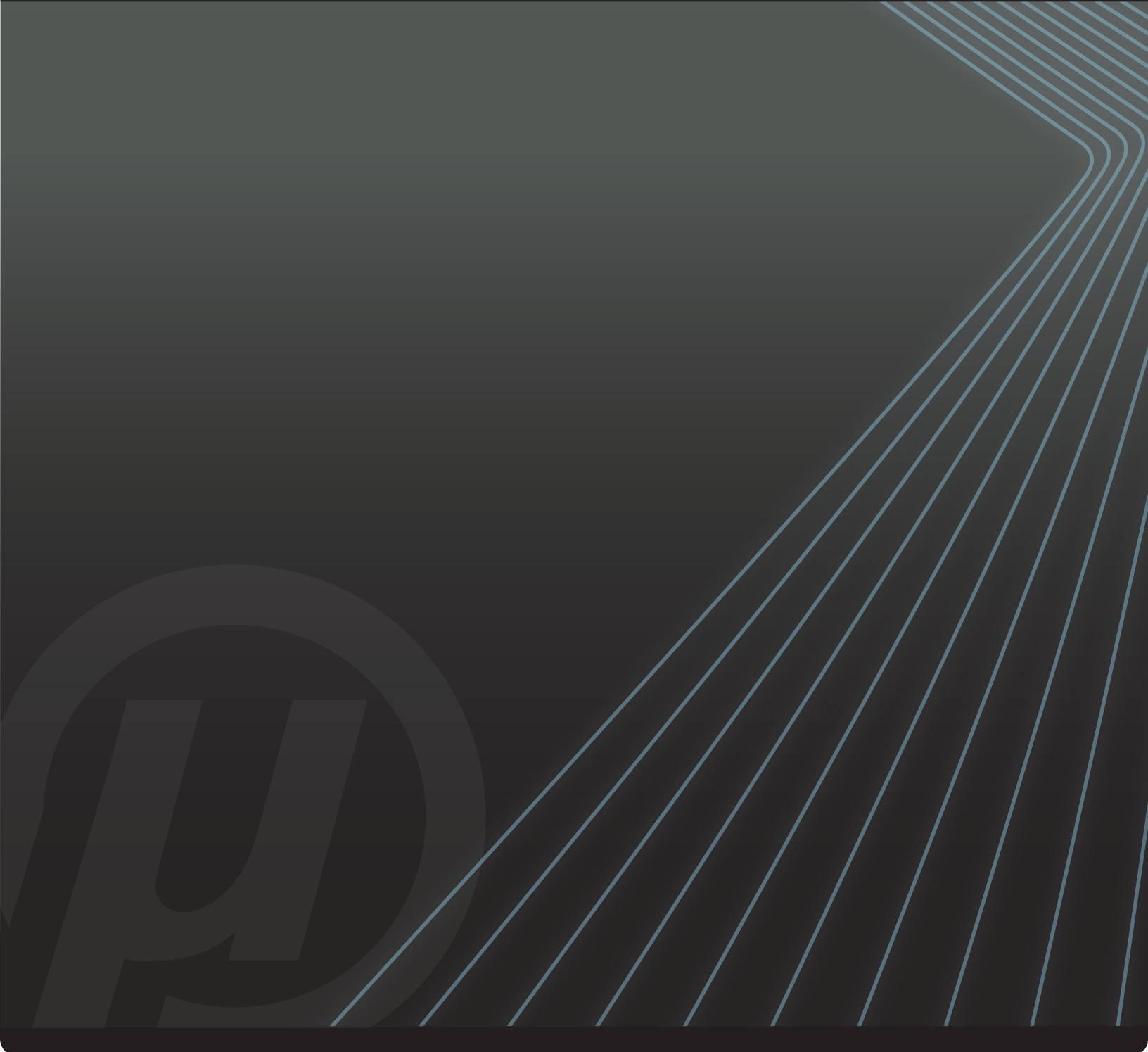




# Mu Dynamics Cyber Range Positioning



## Table of Contents

Corporate Background .....	3
Innovation .....	3
Positioning.....	4
Unique Capabilities brought to IDS/IPS Signature development groups.....	5
Cyber Threat Analysis .....	5
Fuzzing.....	6
DoS (Denial of Service).....	6
Published Vulnerabilities .....	7
Traffic Analysis Toolset – An Example of the Power of Mu Dynamics .....	7
Sophisticated Packet Toolkit: xtractr and pcapr.Local .....	7
Summary .....	10

## Corporate Background

MuDynamics provides a Commercially-available Off-The-Shelf (COTS) Cyber Threat and Active Net-Defense Analysis solution that supports all the efforts of Cyber organizations, from the Floor Analysts to Operations Support, throughout Mission execution. Now, with the unique and salient capabilities of Mu Dynamics Federal solutions, agencies can finally create the digital environment they need to train, evaluate, and develop both offensive and defensive capabilities in their Cyber Range deployments. In addition, the company's Federal solutions give agencies the ability to simulate attacks to assess information assurance capabilities and measure incident response procedures.

With Mu Dynamics Federal solutions, agencies have a robust platform to support their IDS/IPS rule development, verification and validation optimization, and performance analysis. The company can help agencies analyze the efficacy of their rule sets and validate the impact of those rules on the overall infrastructure. Additionally, the Federal performance and security solution can uniquely support Threat Analytics development, by “statefully” recreating any nefarious activity across protocols and OSI layers two through seven. By creating variants of attack vectors, the solution enables agencies to perform variability modeling and simulations that can be used to enhance the development, verification, and validation of their Analytics. Mu Dynamics technology also extends the capabilities of Active-Net Defense, allowing analyst and mission operations personnel to pose as both an “internal” and external threat to recreate Exfiltration strategies.

## Innovation

Mu Dynamics is committed to solving the complex market needs around cyber security testing. Mu Dynamics has led the innovations in the ever-evolving security testing market, offering security testing for any multi-protocol and multi-host application scenario in a common platform. Today, Mu Studio Security is used for security testing at all the leading network operators, including Comcast and Verizon, and largest network equipment manufacturers (NEMs) such as Cisco and Juniper Networks.

The company's Federal solution can uniquely import and test any application or protocol, by converting all multi-host and multi-protocol packet flows into an abstract representation. Because the technology can re-create any packet through the simple modeling of it in the Mu Dynamics domain-specific language, known as the Mu Scenario Language (MuSL), it can be leveraged to do all different forms of testing. As a result, Mu Dynamics can literally model any transaction, even those involving proprietary protocols or previously unseen attack methodologies that might need to be replicated in a Cyber Range.

Because today's security perimeter must block traffic in both directions, Mu Studio Security allows for pass-through testing. This means the same, single test appliance can be used to manage all aspects of a conversation – it can even become up to eight distinct hosts, with arbitrary assignment of client and server roles.

Now, agencies can replicate any attacks or exploits in a Cyber Range and scale them up to test their defenses in a lab setting. Agencies can incorporate all manner of known attacks in their testing. Mu Studio Security enables agencies to use obfuscation, Denial-of-Service simulations, and the delivery of attacks over IPv4, as well as IPv6 environments. It can pair all these test capabilities with a thorough monitoring system, so faults can be correlated with particular test cases to determine exactly what is going on in the digital environment.

Mu Dynamics is recognized as the leading fuzz testing solution, which can be used to identify unknown threats. However, fuzzing is only one aspect of the solution. Combined with Mu Studio Performance, the company's Federal solution can create traffic models that are protocol and transport-agnostic, using auto markup, but still application-aware, to give agencies all the security and performance testing they need within a single platform.

The unique capabilities of Mu Dynamics products are ideally suited for deployment in Cyber Ranges, where the mission is to discover exploits and re-create attacks to get ahead of highly motivated attackers and ensure defenses are robust. Use-cases also include exfiltration testing to ensure that theft of intellectual property and secret information is detected before it leaves the network.

## Positioning

A Cyber Range is a collection of tools and capabilities built in a virtual or physical network or lab designed to help agencies identify new and innovative ways to improve the current infrastructure. They are used to strengthen security, increase stability, and improve the performance of vital government, military, and intelligence network infrastructures.

When the Mu Dynamics Federal solution is integrated into a dedicated Cyber Range, agencies have the latest cutting edge capabilities and tools at their disposal to create unique attacks that can be used to test the cyber security in place. Monitoring these attacks and the behavior of the associated devices allows the engineers to develop and improve the systems used to protect these critical networks. Additionally, attacks specifically targeted at circumventing the security of the network can be performed to aid in the fine-tuning of all these systems. Combined, agencies can improve the overall security of their digital environment and shrink the attack surface, thereby providing fewer areas that can be used to attempt to gain access to these sensitive networks.

With the Mu Dynamics Federal solution used within the Cyber Range, agencies can also test the robustness of the network and its ability to handle large volumes of traffic. Mu Dynamics is capable of generating tests with traffic at volume, which should trigger the network defenses and enable agencies to determine how effective each device is when dealing with different types of attacks, at scale. Sending large volumes of traffic also provides a unique way to measure and improve the overall performance of the network and associated systems, which will help protect against DoS attacks that target the network.

Finally, with the Mu Dynamics Federal solution, the agency can use the Cyber Range to test for the unknown. Through the use of a method known as fuzzing, agencies can find new vulnerabilities and threats that are unknown, to date. A fuzzer is designed to send mutated traffic to targeted machines and monitor how the device or system handles and behaves in the face of these anomalies.

Using the innovative technology offered by Mu Dynamics, agencies will have the tools and capabilities they need to perform exhaustive testing to improve the posture, performance and security of the networks associated with the Cyber Range.

## Unique Capabilities Brought to IDS/IPS Signature Development Groups

Overall Mu Dynamics Federal solution provides some very innovative and unique capabilities to enable a faster and more effective means for creating and validating the performance of the cyber security solutions being employed on the network. Some of the capabilities are highlighted in the following sections.

### *Cyber Threat Analysis*

Agencies need to be able to recreate a scenario and understand what is going on to ensure their network and systems are handling the traffic and performing as expected. There are several different types of tests and analysis agencies can do to determine their cyber threat level. For example, they can perform:

- **Rule Testing and Tuning** – It is important to be able to identify the performance and ability of rules, such as Snort IDS rules, to capture and handle the traffic as expected. The time needed to create a Snort rule is trivial, but the time to test that rule's ability to perform as expected, can be significant.

Mu Dynamics Federal solution dramatically reduces that time, as it only takes moments to create, test, and tune a new rule to get maximum performance. Capturing traffic associated with a specific infection is simple. With Mu Dynamics Federal solution, agencies can import an entire packet capture and hone in on exactly what's happening. Agencies can select the session within the packet capture associated with a beacon (Note, a beacon is the communication between an infected host and a master server, also known as "phoning home.") and quickly alter the packet to create a different, unique beacon to determine exactly what a device will do when it sees the information sent back to the master server. Additionally, the ability to create and use beacons can be used to develop and improve analytics software.

- **Scale Testing** - Agencies need the ability to understand how their systems, services, and applications will handle large traffic loads, as well as how performance will be impacted by certain configurations or changes to a system.

The pioneered ability to generate large volumes of unique, “stateful” traffic to conduct meaningful scale testing. When traffic is not unique or “stateful,” devices can cache responses for given traffic patterns and appear to perform at a higher level than they actually do. With our company’s products and solutions, agencies can run tests with unique, “stateful” traffic that forces the devices to behave as if they would in a production environment. Mu Dynamics products and solutions give agencies the ability to mix different types of traffic and create varying loads for different applications, so agencies can understand exactly how their systems will perform in real-world conditions .

- Insider Threat testing - To secure the network requires understanding the insider threat; this is a person inside the agency network, either an employee or someone who has legitimate physical access, that is trying to remove sensitive information or provide access to an external entity into the network.

Agencies can use the Mu Dynamics Federal solution to take a packet capture and customize the content of a flow to quickly and easily incorporate and hide data. This can then be used to test deep packet inspection systems, as well as data loss prevention solutions, to validate their functionality.

## Fuzzing

Mu Studio Security provides a highly innovative platform that can automatically identify different areas for security testing through a technique known as “fuzzing.” This technique supplies invalid or unexpected inputs to every field, in every packet of an application flow, to precisely identify all the possible and most effective ways to find weaknesses in code as it processes each parameter. Proactively discovering new vulnerabilities gives any cyber defense organization the actionable intelligence they need to prevent an adversary from compromising the organization’s cyber assets.

Mu Studio Security has a knowledge base agencies can leverage that includes all the well-known software fault patterns observed over the last 40 years. The company marries the application or protocol flow with its library of potential vulnerabilities to create an exhaustive set of tests, frequently numbering in the millions (or more). The automation of Mu Studio Security also includes the ability to restart services or devices in the event of a system crash, monitor the Device Under Test (DuT), or any device across the test lab that depends on the DuT, and interact with the system during fuzzing.

The ability to discover, identify and model software flaws can become an important strategic capability for the agency. The fuzzing capabilities of Mu Studio Security are able to automate security testing of any application, protocol or service, including proprietary protocols and custom applications. A Mu Studio Security-equipped Cyber Range is thus able to determine software weaknesses in the same way that attackers do, by sending intentionally malformed inputs to the devices that are exposed on the organization’s security perimeter.

Knowledge is power, and once vulnerabilities are identified, defenses can be built. Agencies can work with their vendors, using the Mu Studio Security purpose-built remediation tools and reports to ensure they can quickly reproduce and then fix any issues that are discovered.

## DoS

Mu Studio Security offers a DoS simulation capability that Cyber Range staff can use to send various types of traffic known to cause DoS attacks to understand how their systems will respond. They can also use these capabilities to identify new ways to try to deny services, if possible, to identify additional weaknesses.

Mu Studio Security can generate test traffic (up to 100,000 packets per second) and provide arbitrary byte-level control over the packet payload and layer-two through four headers to ensure agencies can precisely identify when a problem occurs. Agencies can take advantage of over 50 system templates pre-loaded in the solution to test for known DoS attacks (e.g., Ping of Death, Kiss of Death, SYN flood, Christmas tree, LAND, etc.). They can also easily or customize any DoS attack, using arbitrary (and possibly randomized) packet headers or payloads from layer two through four.

As with fuzzing, the DoS module includes the ability to monitor the DuT to observe any system malfunctions. When a malfunction emerges at a certain traffic threshold, the DoS module will tell the Cyber Range staff how long it takes for the DuT to recover from the attack.

With the reporting and monitoring features of Mu Studio Security it's possible to see areas with a longer response time, as well as determine the resources required for processing the DoS attack. With this information, agencies can calibrate the DoS mitigation at their security perimeter (e.g., Arbor Networks devices) to ensure bad traffic truly is blocked and good traffic permitted.

## Published Vulnerabilities

Mu Studio Security can determine how the agency's network will respond in the face of known threats. Agencies can replay traffic that contains specific triggers from the Common Vulnerabilities and Exposures (CVE) database, as well as other known vulnerabilities, all of which are updated on a monthly basis, to identify where there are weaknesses in their applications and systems.

This is not the same as a vulnerability scanner, such as Retina, Nessus, or IIS, which scan a system for versioning information and then determine where there may be vulnerabilities based on the information they receive. In contrast, Mu Studio Security uses specific triggers, such as a registry key or assembly code, that would be seen inside an attack to identify how the detection and prevention tools would actually handle the attack. As a result, agencies have actionable information on the real vulnerabilities that exist in their systems and network.

The other major benefit of the capabilities of Mu Studio Security is that no exploit is actually being sent. As

compared to exploitation tools, such as Metasploit, Core Impact, or Canvas, that send attacks that can damage the system or leave behind backdoors that can be exploited later, the Mu Studio Security traffic simply appears to be an exploit. The agency can determine how the system will handle the attack when it sees it, but the traffic will never actually attempt to exploit the system.

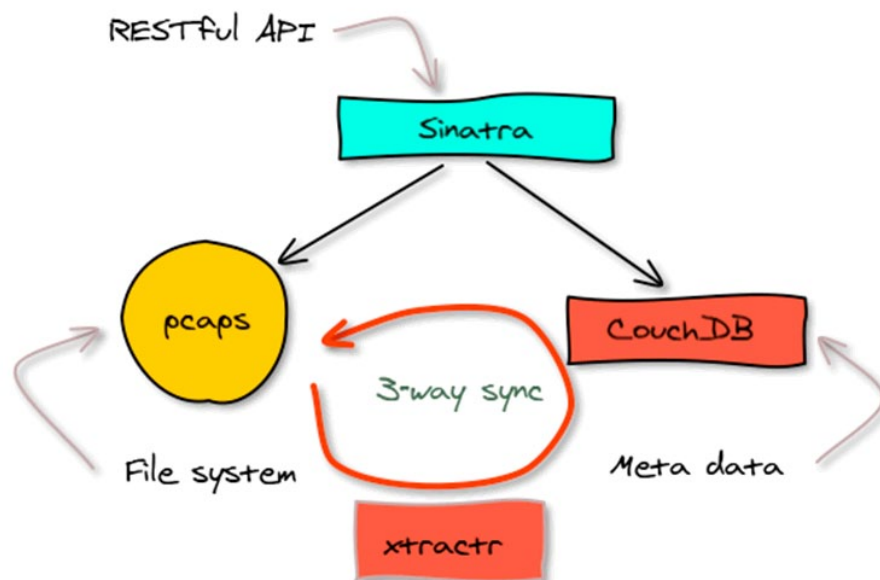
## Traffic Analysis Toolset – An Example of the Power of Mu Dynamics

Mu Dynamics Federal solution offers an extended set of capabilities to support the mission of the Cyber Range, including:

### *Sophisticated Packet Toolkit: xtractr and pcapr.Local*

Xtractr is a hybrid cloud application for indexing, searching, reporting, extracting and collaborating on a large collection of pcaps. This enables agencies to rapidly identify field issues and perform network forensics and troubleshooting with just a few clicks. Answering questions, such as, “Did any DNS queries take more than 2 seconds?” or “Which HTTP GET requests did not use SSL?” is easy.

Xtractr can index up to 10 million packets or 1 gigabyte of pcaps. Mu Dynamics Federal solution has extended xtractr technology in a utility known as pcapr. When you install pcapr.Local, you can index an arbitrary number of packets, limited only by disk space. The relationship of pcapr.Local to xtractr is summarized in this diagram:



Mu Dynamics Federal solution delivers a packet indexing solution that leverages the latest, most powerful software tools, including the NoSQL database, “CouchDB,” accessible via RESTful. This enables agencies to create their own queries to manipulate their packets with the same powerful web-based software tools they are used to using.

The searching and reporting capability is known as “nuggets,” which allows agencies to create queries on the data and define reports. Nuggets are search strings that are easily shared among users, so they can look for interesting forensic evidence or field issues in large collections of pcaps -in other words, nuggets make it easy to find a needle in a haystack. Some predefined nuggets are built into Mu Dynamics Federal solution, but users can optionally upload their own nuggets if they so choose to quickly and easily extract the information that is most relevant to them from the packet captures.

**BETA** This index has #352 hosts, #17 services, #501 flows and #4511 packets.

Hosts Flows Packets Fields Labels Nuggets

label id	time	packets	src	sport	dst	dport	service	title
▶ label 1.	0.0000	23	192.168.5.140	50825	74.85.18.166	443	TLSv1	Application Data
▶ label 2.	0.0330	6	2001:0:4137:9e76:3894:3fba:bf79:bcc6	49221	2001:0:5ef5:79fd:1471:35a7:a977:f158	3544	IPv6	IPv6 no next header
▶ label 3.	0.0411	7	192.168.5.219	52026	77.250.217.161	51413	BitTorrent	Handshake
▶ label 4.	0.0523	3	92.119.148.174	63245	192.168.5.219	52342	UDP	Source port: 63245 Destination port
▶ label 5.	0.0571	987	2.33.6.175	43543	192.168.5.219	52342	UDP	Source port: 43543 Destination port
▶ label 6.	0.0656	8	63.131.144.203	443	192.168.5.219	52018	SSL	Continuation Data
▶ label 7.	0.0732	10	192.168.5.219	52019	63.131.144.203	443	TLSv1	Client Key Exchange, Change Cipt
▶ label 8.	0.1102	71	192.168.5.219	52342	61.109.100.147	21292	UDP	Source port: 52342 Destination port
▶ label 9.	0.1850	24	192.168.5.219	52342	86.136.14.167	22930	UDP	Source port: 52342 Destination port
▶ label 10.	0.1850	2	192.168.5.219	52342	86.135.93.99	34457	UDP	Source port: 52342 Destination port
▶ label 11.	0.1881	7	192.168.5.219	51466	200.82.81.137	80	HTTP	GET /bannerscript.aspx?TargetZon
▶ label 12.	0.1884	7	192.168.5.219	51472	200.82.81.137	80	HTTP	GET /bannerscript.aspx?TargetZon
▶ label 13.	0.1969	24	192.168.5.219	51474	200.82.81.137	80	HTTP	GET /Files/download.aspx?id=130
▶ label 14.	0.1975	9	192.168.5.219	51471	200.82.81.137	80	HTTP	GET /Files/download.aspx?id=129
▶ label 15.	0.1983	7	192.168.5.219	51475	200.82.81.137	80	HTTP	GET /Files/download.aspx?id=129
▶ label 16.	0.1990	7	192.168.5.219	51473	200.82.81.137	80	HTTP	GET /Files/download.aspx?id=127
▶ label 17.	0.2196	2	192.168.5.219	51405	192.168.5.1	53	DNS	Standard query A twitter.com
▶ label 18.	0.2200	2	192.168.5.219	49834	192.168.5.1	53	DNS	Standard query A www.facebook.c
▶ label 19.	0.2889	678	188.69.227.236	45682	192.168.5.219	52342	UDP	Source port: 45682 Destination port
▶ label 20.	0.3145	13	174.54.41.70	64828	192.168.5.219	49221	UDP	Source port: 64828 Destination port

▶more

## An example nugget is:

```
flow.service:HTTP> count('http.user.agent', { title: "Top Web Browsers", limit:10 })
```

It is easy to see how an agency could use it below to create a chart of the top HTTP user agents in the pcap index:



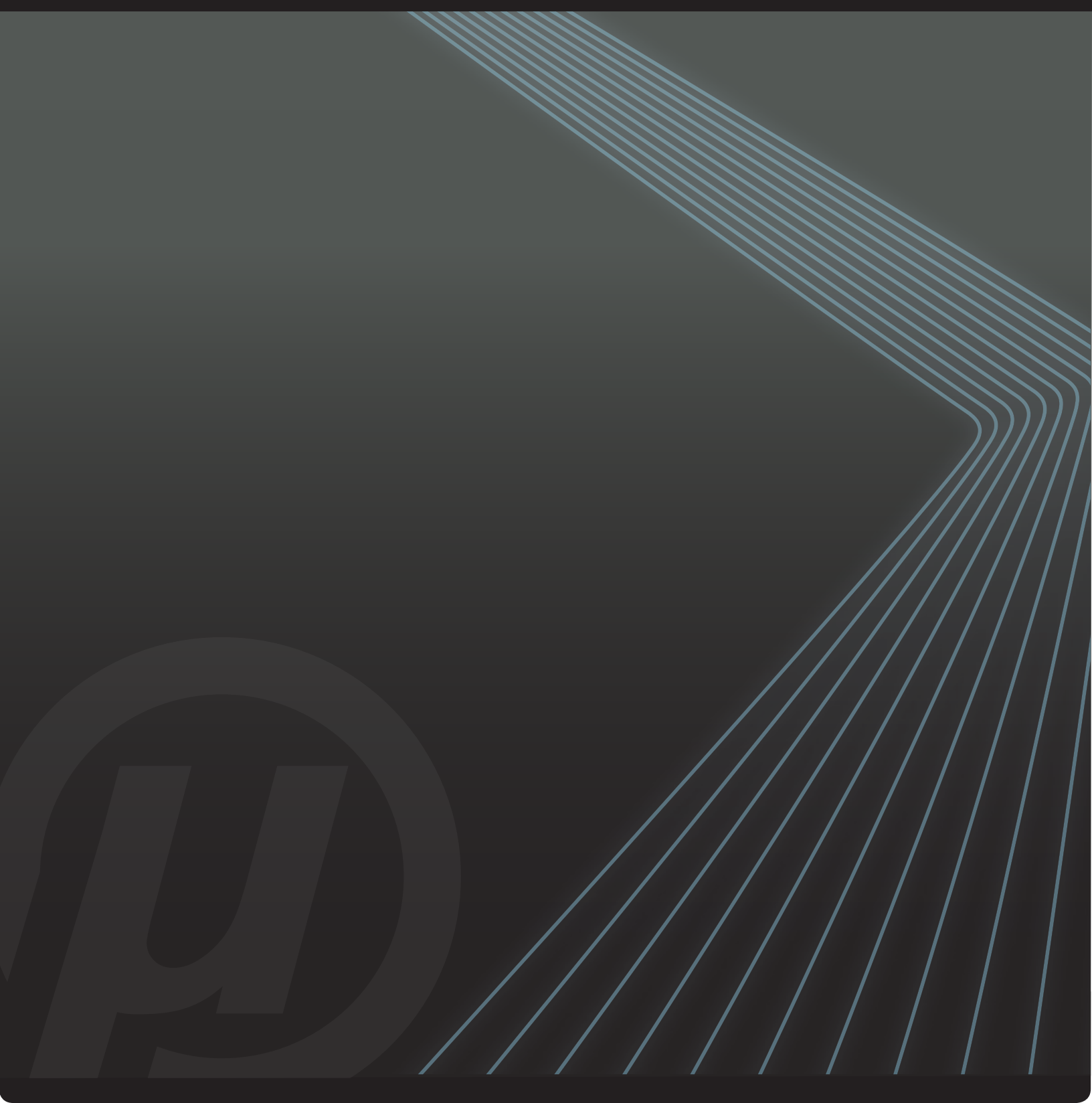
This nugget could be very useful for forensics, enabling the agency to quickly determine the web browser and narrow down the operating system in use.

The nugget query layout is as follows:

1. First field is for narrowing which packets to search through.
2. The > is to define what specifically to search for within said packets.
3. Next is the action to perform - in this case count. This field requires a parameter to perform the action on.
4. The title is an optional field to enable you to label the chart.
5. Finally the limit field is to limit the number of results - in this case, it's the top 10.
6. With the search terms you can include some additional options such as: negation, ranges, time slices, less than, this or that aka OR statement.

## Summary

With Mu Dynamics, agencies can create the digital environment they need to identify, evaluate, and develop both offensive and defensive capabilities in their Cyber Range deployments. Only Mu Dynamics provides a single platform that can be leveraged to do all different forms of testing. The ability to model any transaction, even those involving proprietary protocols or previously unseen attack methodologies that might need to be replicated in a Cyber Range, gives agencies unprecedented visibility into the potential weaknesses of their applications and systems. By being able to simulate attacks, agencies can assess their security posture, information assurance capabilities, and incident response procedures. They can then take the remediation tools and reports generated by Mu Dynamics to resolve any issues that are uncovered. In sum, Mu Dynamics, Inc. provides agencies the tools and knowledge they need to strengthen their defenses and maximize the performance of their applications and network infrastructure.



**Web:** [www.mudynamics.com](http://www.mudynamics.com)

**Address:** 800 W. California Avenue, Sunnyvale, CA 94086, USA

**Phone:** 866-276-4640 or 408-329-6330

**Fax:** 408-329-6317

Copyright © 2011 Mu Dynamics. All rights reserved. Mu Dynamics, Mu Studio Performance, Mu Studio Security, Mu-8000, Mu Dynamics logo, and Innovate with Confidence are trademarks of Mu Dynamics.