Cyber Gyan Virtual Internship Program

Centre for Development of Advanced Computing (CDAC), Noida

Submitted By:

Priyanka Lotiya

Project Trainee, (May-July) 2025

Traffic Monitoring Use Cases Using Network Monitoring Tools and Their Installation

Cyber Security / Network Traffic Analysis

Tools: Security Onion, Arkime, Wireshark

Duration: 19 May – 26 May 2025

PROBLEM STATEMENT

With increasing cyber threats, it is critical to monitor network traffic for anomalies, malicious patterns, and performance issues.

Lack of proper traffic inspection can result in missed intrusions, malware infections, or policy violations.

TECHNOLOGY/TOOLS TO BE USED

Tool	Purpose
Security Onion	IDS/IPS, Packet Capture, Alerts
Arkime (Moloch)	Full packet capture and traffic analysis
Wireshark	Deep packet inspection (PCAP)
VirtualBox/VM	For setting up isolated testing lab

ABOUT THE TOPIC

- Traffic Monitoring is the process of capturing and analyzing network packets to understand communication patterns.
- Helps detect threats like:
  - Port scans
  - Suspicious DNS queries
  - Malicious payloads
  - Policy violations

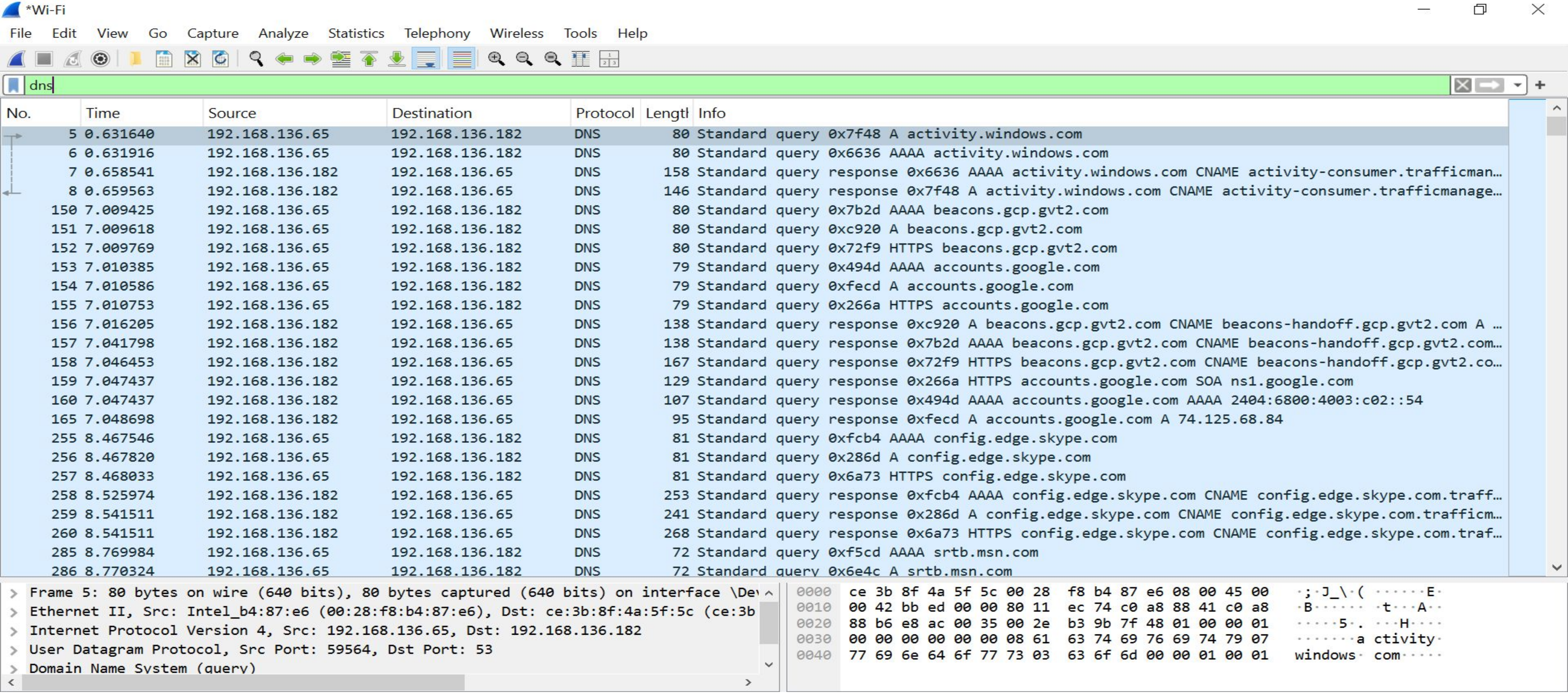
WHY THIS PROBLEM OCCURS

- Increasing network complexity and encrypted traffic
- Lack of trained personnel and proactive detection systems
- Not all organizations use intrusion detection tools
- Manual inspection is inefficient and slow

SOLUTIONS / COUNTERMEASURES

- Deploy **Security Onion** for real-time alerts using Suricata and Zeek
- Use **Arkime** to analyze historical PCAPs
- Regularly review DNS/HTTP logs
- Integrate tools with **SIEM (ELK/Splunk)**
- Train security teams to identify Indicators of Compromise (IoCs)

IMPLEMENTATION SNAPSHOTS

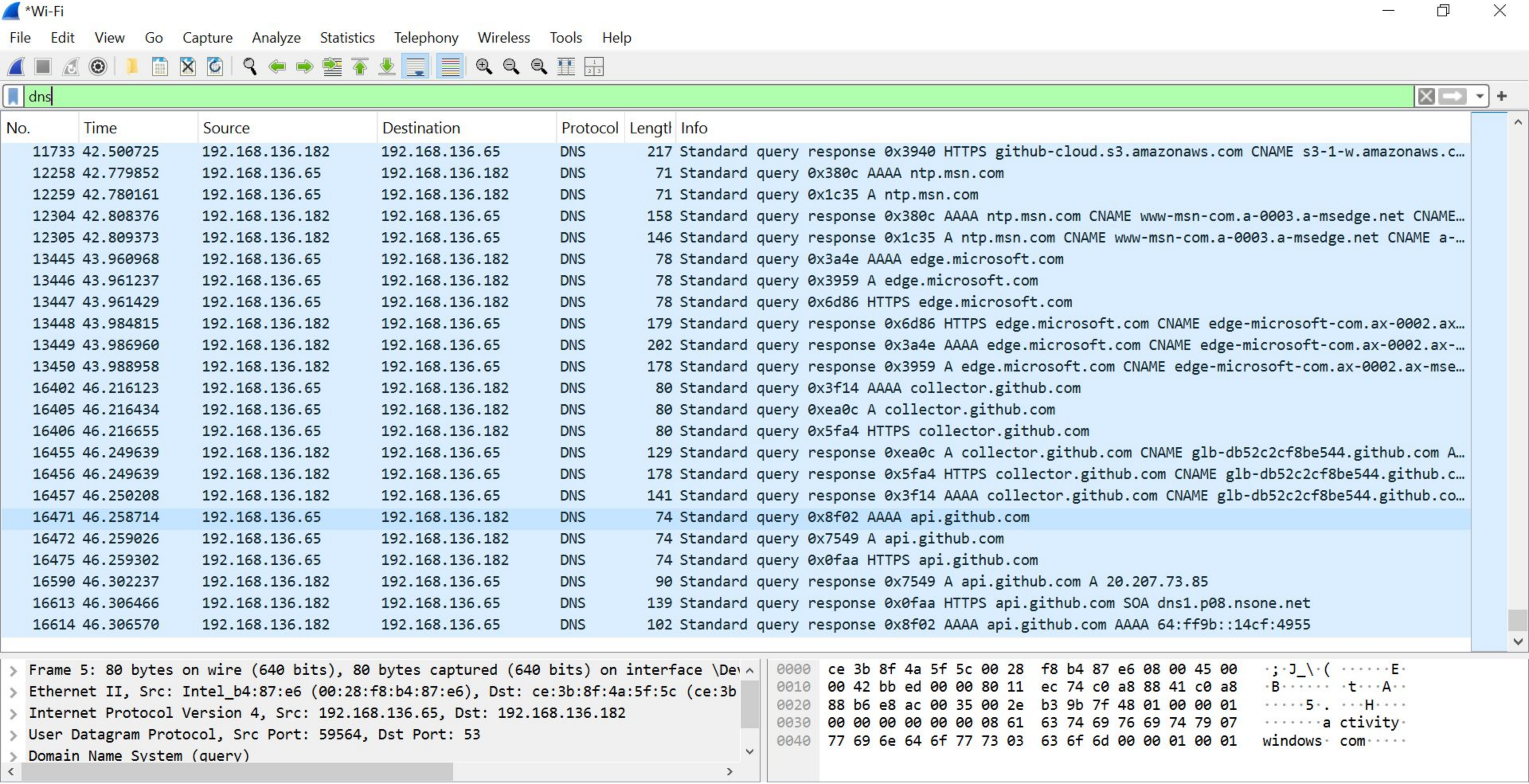


dns

No.	Time	Source	Destination	Protocol	Lengtl	Info
5	0.631640	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x7f48 A activity.windows.com
6	0.631916	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x6636 AAAA activity.windows.com
7	0.658541	192.168.136.182	192.168.136.65	DNS	158	Standard query response 0x6636 AAAA activity.windows.com CNAME activity-consumer.trafficman…
8	0.659563	192.168.136.182	192.168.136.65	DNS	146	Standard query response 0x7f48 A activity.windows.com CNAME activity-consumer.trafficmanage…
150	7.009425	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x7b2d AAAA beacons.gcp.gvt2.com
151	7.009618	192.168.136.65	192.168.136.182	DNS	80	Standard query 0xc920 A beacons.gcp.gvt2.com
152	7.009769	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x72f9 HTTPS beacons.gcp.gvt2.com
153	7.010385	192.168.136.65	192.168.136.182	DNS	79	Standard query 0x494d AAAA accounts.google.com
154	7.010586	192.168.136.65	192.168.136.182	DNS	79	Standard query 0xfecd A accounts.google.com
155	7.010753	192.168.136.65	192.168.136.182	DNS	79	Standard query 0x266a HTTPS accounts.google.com
156	7.016205	192.168.136.182	192.168.136.65	DNS	138	Standard query response 0xc920 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A …
157	7.041798	192.168.136.182	192.168.136.65	DNS	138	Standard query response 0x7b2d AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com…
158	7.046453	192.168.136.182	192.168.136.65	DNS	167	Standard query response 0x72f9 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.co…
159	7.047437	192.168.136.182	192.168.136.65	DNS	129	Standard query response 0x266a HTTPS accounts.google.com SOA ns1.google.com
160	7.047437	192.168.136.182	192.168.136.65	DNS	107	Standard query response 0x494d AAAA accounts.google.com AAAA 2404:6800:4003:c02::54
165	7.048698	192.168.136.182	192.168.136.65	DNS	95	Standard query response 0xfecd A accounts.google.com A 74.125.68.84
255	8.467546	192.168.136.65	192.168.136.182	DNS	81	Standard query 0xfcb4 AAAA config.edge.skype.com
256	8.467820	192.168.136.65	192.168.136.182	DNS	81	Standard query 0x286d A config.edge.skype.com
257	8.468033	192.168.136.65	192.168.136.182	DNS	81	Standard query 0x6a73 HTTPS config.edge.skype.com
258	8.525974	192.168.136.182	192.168.136.65	DNS	253	Standard query response 0xfcb4 AAAA config.edge.skype.com CNAME config.edge.skype.com.traff…
259	8.541511	192.168.136.182	192.168.136.65	DNS	241	Standard query response 0x286d A config.edge.skype.com CNAME config.edge.skype.com.trafficm…
260	8.541511	192.168.136.182	192.168.136.65	DNS	268	Standard query response 0x6a73 HTTPS config.edge.skype.com CNAME config.edge.skype.com.traf…
285	8.769984	192.168.136.65	192.168.136.182	DNS	72	Standard query 0xf5cd AAAA srtb.msn.com
286	8.770324	192.168.136.65	192.168.136.182	DNS	72	Standard query 0x6e4c A srtb.msn.com

```
> Frame 5: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \De
> Ethernet II, Src: Intel_b4:87:e6 (00:28:f8:b4:87:e6), Dst: ce:3b:8f:4a:5f:5c (ce:3b
> Internet Protocol Version 4, Src: 192.168.136.65, Dst: 192.168.136.182
> User Datagram Protocol, Src Port: 59564, Dst Port: 53
> Domain Name System (query)
```

```
0000  ce 3b 8f 4a 5f 5c 00 28  f8 b4 87 e6 08 00 45 00   ·;·J_\·( ······E·
0010  00 42 bb ed 00 00 80 11  ec 74 c0 a8 88 41 c0 a8   ·B······ ·t···A··
0020  88 b6 e8 ac 00 35 00 2e  b3 9b 7f 48 01 00 00 01   ·····5·. ···H····
0030  00 00 00 00 00 00 08 61  63 74 69 76 69 74 79 07   ·······a ctivity·
0040  77 69 6e 64 6f 77 73 03  63 6f 6d 00 00 01 00 01   windows· com·····
```

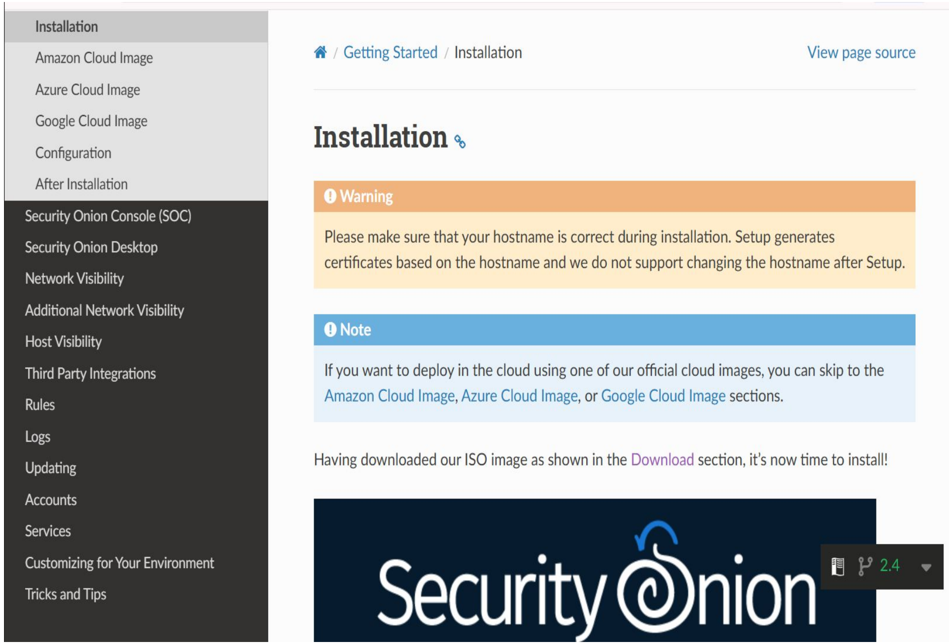


dns

No.	Time	Source	Destination	Protocol	Lengtl	Info
11733	42.500725	192.168.136.182	192.168.136.65	DNS	217	Standard query response 0x3940 HTTPS github-cloud.s3.amazonaws.com CNAME s3-1-w.amazonaws.c…
12258	42.779852	192.168.136.65	192.168.136.182	DNS	71	Standard query 0x380c AAAA ntp.msn.com
12259	42.780161	192.168.136.65	192.168.136.182	DNS	71	Standard query 0x1c35 A ntp.msn.com
12304	42.808376	192.168.136.182	192.168.136.65	DNS	158	Standard query response 0x380c AAAA ntp.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME…
12305	42.809373	192.168.136.182	192.168.136.65	DNS	146	Standard query response 0x1c35 A ntp.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-…
13445	43.960968	192.168.136.65	192.168.136.182	DNS	78	Standard query 0x3a4e AAAA edge.microsoft.com
13446	43.961237	192.168.136.65	192.168.136.182	DNS	78	Standard query 0x3959 A edge.microsoft.com
13447	43.961429	192.168.136.65	192.168.136.182	DNS	78	Standard query 0x6d86 HTTPS edge.microsoft.com
13448	43.984815	192.168.136.182	192.168.136.65	DNS	179	Standard query response 0x6d86 HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax…
13449	43.986960	192.168.136.182	192.168.136.65	DNS	202	Standard query response 0x3a4e AAAA edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-…
13450	43.988958	192.168.136.182	192.168.136.65	DNS	178	Standard query response 0x3959 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-mse…
16402	46.216123	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x3f14 AAAA collector.github.com
16405	46.216434	192.168.136.65	192.168.136.182	DNS	80	Standard query 0xea0c A collector.github.com
16406	46.216655	192.168.136.65	192.168.136.182	DNS	80	Standard query 0x5fa4 HTTPS collector.github.com
16455	46.249639	192.168.136.182	192.168.136.65	DNS	129	Standard query response 0xea0c A collector.github.com CNAME glb-db52c2cf8be544.github.com A…
16456	46.249639	192.168.136.182	192.168.136.65	DNS	178	Standard query response 0x5fa4 HTTPS collector.github.com CNAME glb-db52c2cf8be544.github.c…
16457	46.250208	192.168.136.182	192.168.136.65	DNS	141	Standard query response 0x3f14 AAAA collector.github.com CNAME glb-db52c2cf8be544.github.co…
16471	46.258714	192.168.136.65	192.168.136.182	DNS	74	Standard query 0x8f02 AAAA api.github.com
16472	46.259026	192.168.136.65	192.168.136.182	DNS	74	Standard query 0x7549 A api.github.com
16475	46.259302	192.168.136.65	192.168.136.182	DNS	74	Standard query 0x0faa HTTPS api.github.com
16590	46.302237	192.168.136.182	192.168.136.65	DNS	90	Standard query response 0x7549 A api.github.com A 20.207.73.85
16613	46.306466	192.168.136.182	192.168.136.65	DNS	139	Standard query response 0x0faa HTTPS api.github.com SOA dns1.p08.nsone.net
16614	46.306570	192.168.136.182	192.168.136.65	DNS	102	Standard query response 0x8f02 AAAA api.github.com AAAA 64:ff9b::14cf:4955

```
> Frame 5: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \De
> Ethernet II, Src: Intel_b4:87:e6 (00:28:f8:b4:87:e6), Dst: ce:3b:8f:4a:5f:5c (ce:3b
> Internet Protocol Version 4, Src: 192.168.136.65, Dst: 192.168.136.182
> User Datagram Protocol, Src Port: 59564, Dst Port: 53
> Domain Name System (query)
```

```
0000  ce 3b 8f 4a 5f 5c 00 28  f8 b4 87 e6 08 00 45 00   ·;·J_\·( ······E·
0010  00 42 bb ed 00 00 80 11  ec 74 c0 a8 88 41 c0 a8   ·B······ ·t···A··
0020  88 b6 e8 ac 00 35 00 2e  b3 9b 7f 48 01 00 00 01   ·····5·. ···H····
0030  00 00 00 00 00 00 08 61  63 74 69 76 69 74 79 07   ·······a ctivity·
0040  77 69 6e 64 6f 77 73 03  63 6f 6d 00 00 01 00 01   windows· com·····
```



Installation
Amazon Cloud Image
Azure Cloud Image
Google Cloud Image
Configuration
After Installation
Security Onion Console (SOC)
Security Onion Desktop
Network Visibility
Additional Network Visibility
Host Visibility
Third Party Integrations
Rules
Logs
Updating
Accounts
Services
Customizing for Your Environment
Tricks and Tips

/ Getting Started / Installation — View page source

Installation

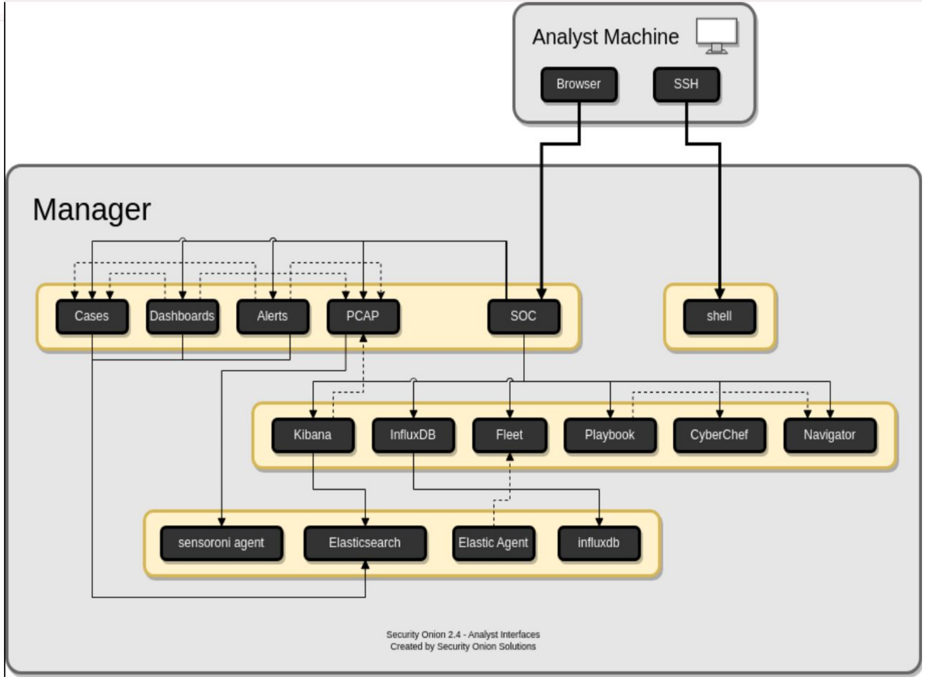
Warning

Please make sure that your hostname is correct during installation. Setup generates certificates based on the hostname and we do not support changing the hostname after Setup.

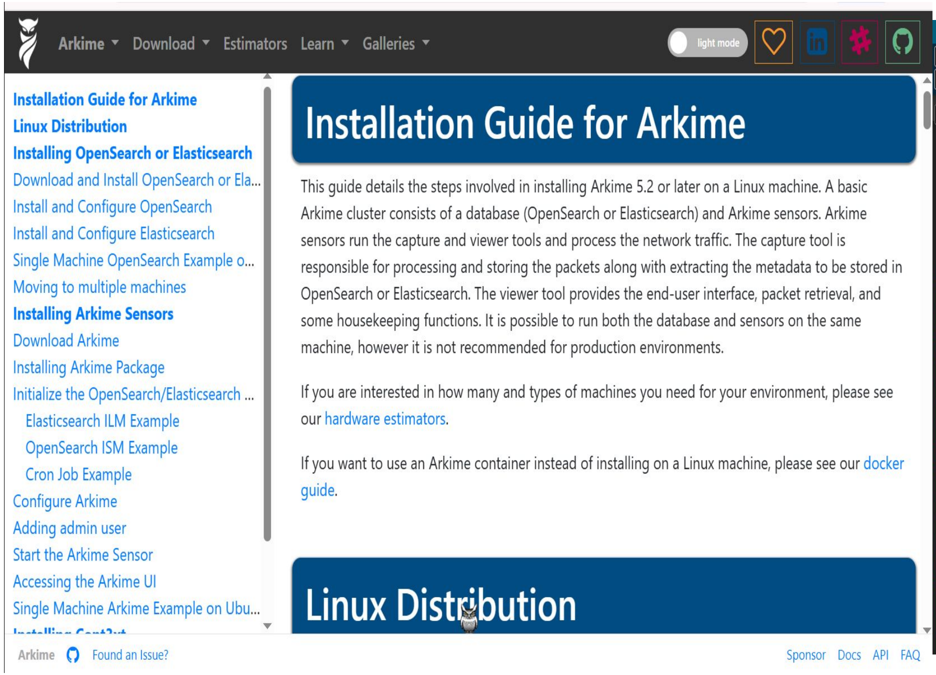
Note

If you want to deploy in the cloud using one of our official cloud images, you can skip to the Amazon Cloud Image, Azure Cloud Image, or Google Cloud Image sections.

Having downloaded our ISO image as shown in the Download section, it's now time to install!



Security Onion 2.4 - Analyst Interfaces
Created by Security Onion Solutions



- Installation Guide for Arkime
- Linux Distribution
- Installing OpenSearch or Elasticsearch
- Download and Install OpenSearch or Ela...
- Install and Configure OpenSearch
- Install and Configure Elasticsearch
- Single Machine OpenSearch Example o...
- Moving to multiple machines
- Installing Arkime Sensors
- Download Arkime
- Installing Arkime Package
- Initialize the OpenSearch/Elasticsearch ...
  - Elasticsearch ILM Example
  - OpenSearch ISM Example
  - Cron Job Example
- Configure Arkime
- Adding admin user
- Start the Arkime Sensor
- Accessing the Arkime UI
- Single Machine Arkime Example on Ubu...

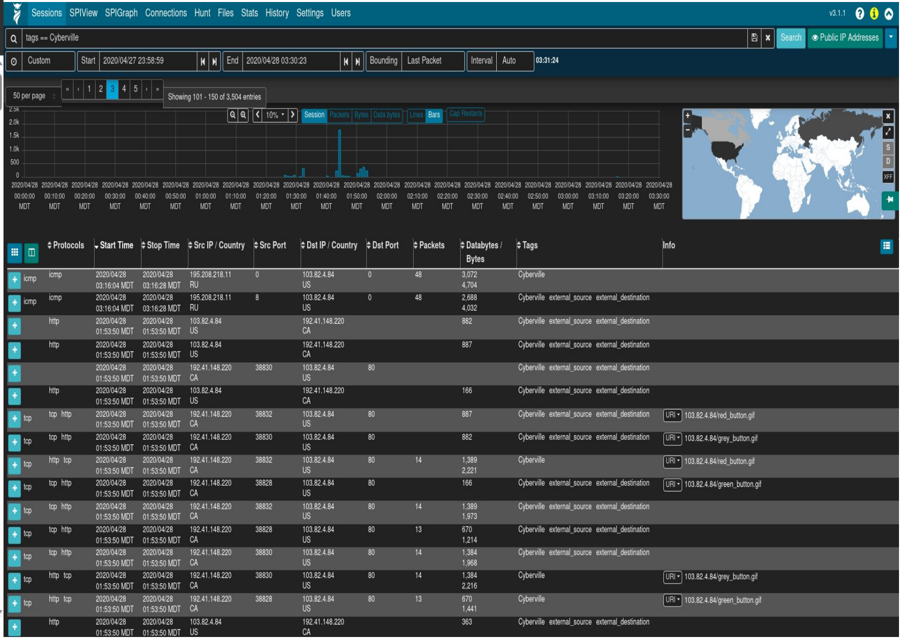
Installation Guide for Arkime

This guide details the steps involved in installing Arkime 5.2 or later on a Linux machine. A basic Arkime cluster consists of a database (OpenSearch or Elasticsearch) and Arkime sensors. Arkime sensors run the capture and viewer tools and process the network traffic. The capture tool is responsible for processing and storing the packets along with extracting the metadata to be stored in OpenSearch or Elasticsearch. The viewer tool provides the end-user interface, packet retrieval, and some housekeeping functions. It is possible to run both the database and sensors on the same machine, however it is not recommended for production environments.

If you are interested in how many and types of machines you need for your environment, please see our hardware estimators.

If you want to use an Arkime container instead of installing on a Linux machine, please see our docker guide.

Linux Distribution



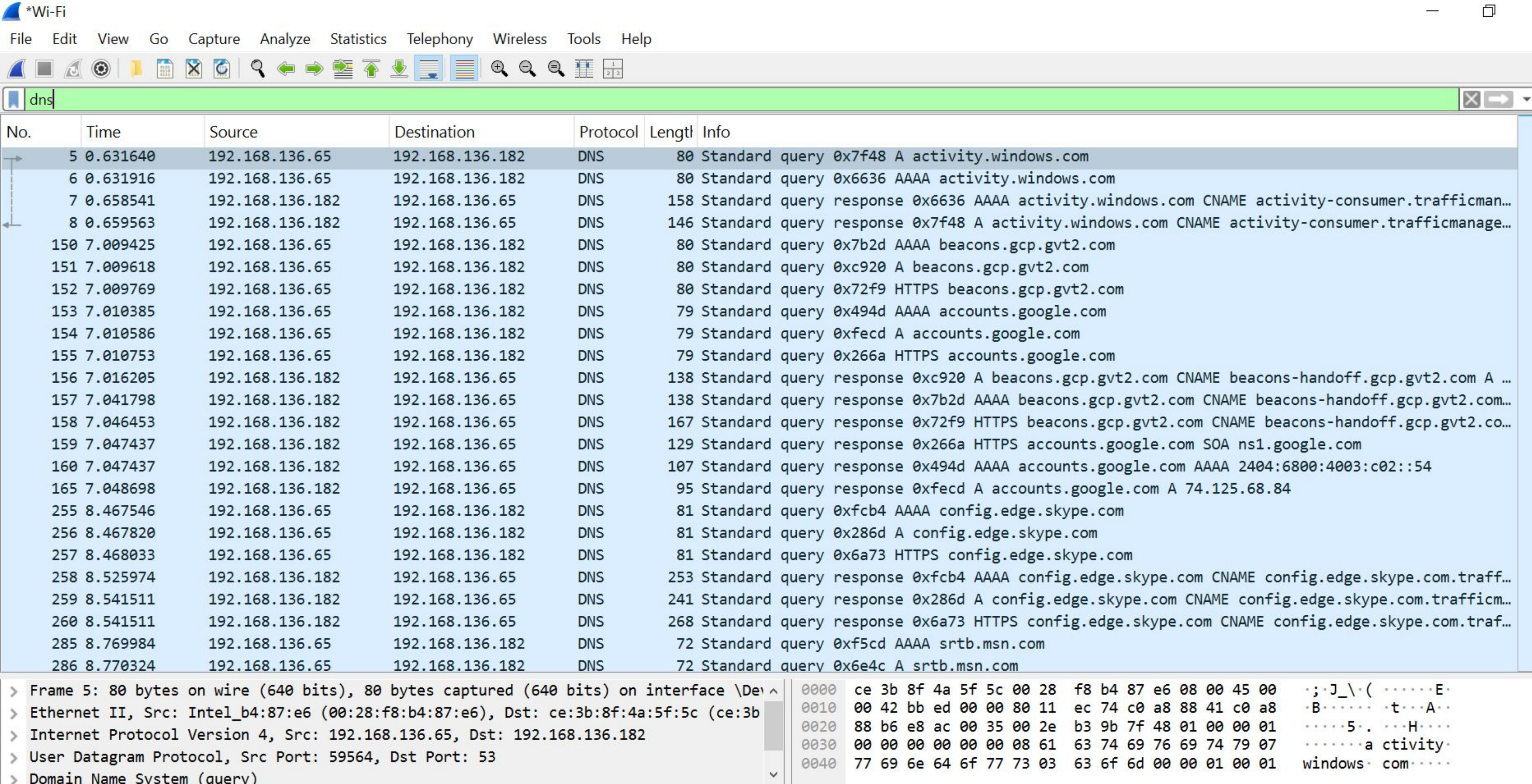
tags == Cyberville

Custom | Start 2020/04/27 23:58:59 | End 2020/04/28 03:30:23 | Bounding Last Packet | Interval Auto | 03:31:24

50 per page

Showing 101 - 150 of 3,504 entries

	Protocols	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Tags	Info
icmp	icmp	2020/04/28 03:16:04 MDT	2020/04/28 03:16:28 MDT	195.208.218.11 RU	0	103.82.4.84 US	0	48	3,072 4,704	Cyberville	
icmp	icmp	2020/04/28 03:16:04 MDT	2020/04/28 03:16:28 MDT	195.208.218.11 RU	8	103.82.4.84 US	0	48	2,688 4,032	Cyberville external_source external_destination	
	http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	103.82.4.84 US		192.41.148.220 CA			882	Cyberville external_source external_destination	
	http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	103.82.4.84 US		192.41.148.220 CA			887	Cyberville external_source external_destination	
		2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38830	103.82.4.84 US	80			Cyberville external_source external_destination	
	http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	103.82.4.84 US		192.41.148.220 CA			166	Cyberville external_source external_destination	
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38832	103.82.4.84 US	80		887	Cyberville external_source external_destination	URI 103.82.4.84/red_button.gif
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38830	103.82.4.84 US	80		882	Cyberville external_source external_destination	URI 103.82.4.84/grey_button.gif
tcp	http tcp	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38832	103.82.4.84 US	80	14	1,389 2,221	Cyberville	URI 103.82.4.84/red_button.gif
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38828	103.82.4.84 US	80		166	Cyberville external_source external_destination	URI 103.82.4.84/green_button.gif
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38832	103.82.4.84 US	80	14	1,389 1,973	Cyberville external_source external_destination	
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38828	103.82.4.84 US	80	13	670 1,214	Cyberville external_source external_destination	
tcp	tcp http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38830	103.82.4.84 US	80	14	1,384 1,968	Cyberville external_source external_destination	
tcp	http tcp	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38830	103.82.4.84 US	80	14	1,384 2,216	Cyberville	URI 103.82.4.84/grey_button.gif
tcp	http tcp	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	192.41.148.220 CA	38828	103.82.4.84 US	80	13	670 1,441	Cyberville	URI 103.82.4.84/green_button.gif
	http	2020/04/28 01:53:50 MDT	2020/04/28 01:53:50 MDT	103.82.4.84 US		192.41.148.220 CA			363	Cyberville external_source external_destination	



dns

```
No.    Time       Source           Destination      Protocol Lengtł Info
     5 0.631640   192.168.136.65   192.168.136.182  DNS        80 Standard query 0x7f48 A activity.windows.com
     6 0.631916   192.168.136.65   192.168.136.182  DNS        80 Standard query 0x6636 AAAA activity.windows.com
     7 0.658541   192.168.136.182  192.168.136.65   DNS       158 Standard query response 0x6636 AAAA activity.windows.com CNAME activity-consumer.trafficman…
     8 0.659563   192.168.136.182  192.168.136.65   DNS       146 Standard query response 0x7f48 A activity.windows.com CNAME activity-consumer.trafficmanage…
   150 7.009425   192.168.136.65   192.168.136.182  DNS        80 Standard query 0x7b2d AAAA beacons.gcp.gvt2.com
   151 7.009618   192.168.136.65   192.168.136.182  DNS        80 Standard query 0xc920 A beacons.gcp.gvt2.com
   152 7.009769   192.168.136.65   192.168.136.182  DNS        80 Standard query 0x72f9 HTTPS beacons.gcp.gvt2.com
   153 7.010385   192.168.136.65   192.168.136.182  DNS        79 Standard query 0x494d AAAA accounts.google.com
   154 7.010586   192.168.136.65   192.168.136.182  DNS        79 Standard query 0xfecd A accounts.google.com
   155 7.010753   192.168.136.65   192.168.136.182  DNS        79 Standard query 0x266a HTTPS accounts.google.com
   156 7.016205   192.168.136.182  192.168.136.65   DNS       138 Standard query response 0xc920 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A …
   157 7.041798   192.168.136.182  192.168.136.65   DNS       138 Standard query response 0x7b2d AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com…
   158 7.046453   192.168.136.182  192.168.136.65   DNS       167 Standard query response 0x72f9 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.co…
   159 7.047437   192.168.136.182  192.168.136.65   DNS       129 Standard query response 0x266a HTTPS accounts.google.com SOA ns1.google.com
   160 7.047437   192.168.136.182  192.168.136.65   DNS       107 Standard query response 0x494d AAAA accounts.google.com AAAA 2404:6800:4003:c02::54
   165 7.048698   192.168.136.182  192.168.136.65   DNS        95 Standard query response 0xfecd A accounts.google.com A 74.125.68.84
   255 8.467546   192.168.136.65   192.168.136.182  DNS        81 Standard query 0xfcb4 AAAA config.edge.skype.com
   256 8.467820   192.168.136.65   192.168.136.182  DNS        81 Standard query 0x286d A config.edge.skype.com
   257 8.468033   192.168.136.65   192.168.136.182  DNS        81 Standard query 0x6a73 HTTPS config.edge.skype.com
   258 8.525974   192.168.136.182  192.168.136.65   DNS       253 Standard query response 0xfcb4 AAAA config.edge.skype.com CNAME config.edge.skype.com.traff…
   259 8.541511   192.168.136.182  192.168.136.65   DNS       241 Standard query response 0x286d A config.edge.skype.com CNAME config.edge.skype.com.trafficm…
   260 8.541511   192.168.136.182  192.168.136.65   DNS       268 Standard query response 0x6a73 HTTPS config.edge.skype.com CNAME config.edge.skype.com.traf…
   285 8.769984   192.168.136.65   192.168.136.182  DNS        72 Standard query 0xf5cd AAAA srtb.msn.com
   286 8.770324   192.168.136.65   192.168.136.182  DNS        72 Standard query 0x6e4c A srtb.msn.com
```

```
> Frame 5: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Dev
> Ethernet II, Src: Intel_b4:87:e6 (00:28:f8:b4:87:e6), Dst: ce:3b:8f:4a:5f:5c (ce:3b
> Internet Protocol Version 4, Src: 192.168.136.65, Dst: 192.168.136.182
> User Datagram Protocol, Src Port: 59564, Dst Port: 53
> Domain Name System (query)
```

```
0000  ce 3b 8f 4a 5f 5c 00 28  f8 b4 87 e6 08 00 45 00   ·;·J_\·( ······E·
0010  00 42 bb ed 00 00 80 11  ec 74 c0 a8 88 41 c0 a8   ·B······ ·t···A··
0020  88 b6 e8 ac 00 35 00 2e  b3 9b 7f 48 01 00 00 01   ·····5·. ···H····
0030  00 00 00 00 00 00 08 61  63 74 69 76 69 74 79 07   ·······a ctivity·
0040  77 69 6e 64 6f 77 73 03  63 6f 6d 00 00 01 00 01   windows· com·····
```

LEARNING OUTCOMES

- Understood how to install and use monitoring tools
- Gained practical experience analyzing traffic data
- Learned how to identify and interpret suspicious network behavior
- Explored IoCs and their real-world relevance

THANK YOU!

Priyanka Lotiya

CDAC Cyber Gyan Internship

(May–July 2025)