

Pontifícia Universidade Católica do Rio Grande do Sul
Laboratório de Redes de Computadores
Engenharia de Software

Carolina Ferreira e Mateus Caçabuena

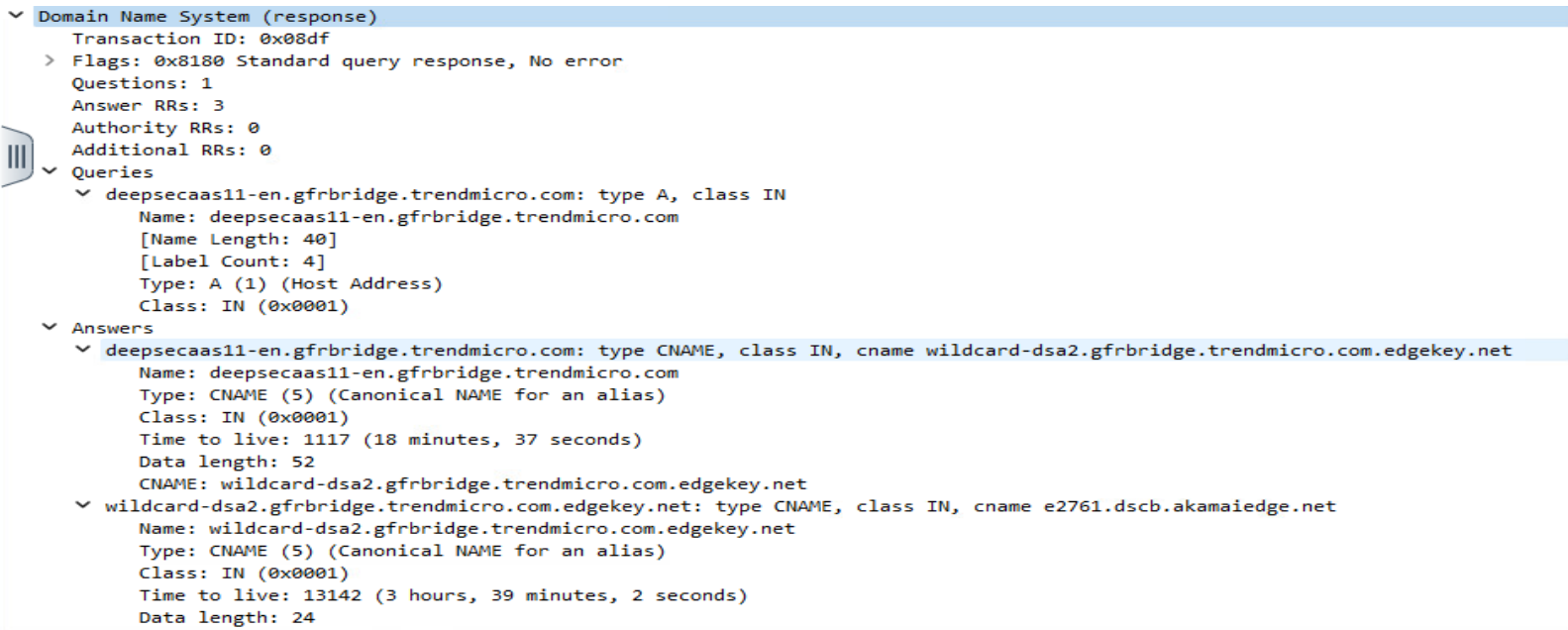
Relatório da Monitoração de Protocolos de Aplicação

Porto Alegre

2024

DNS

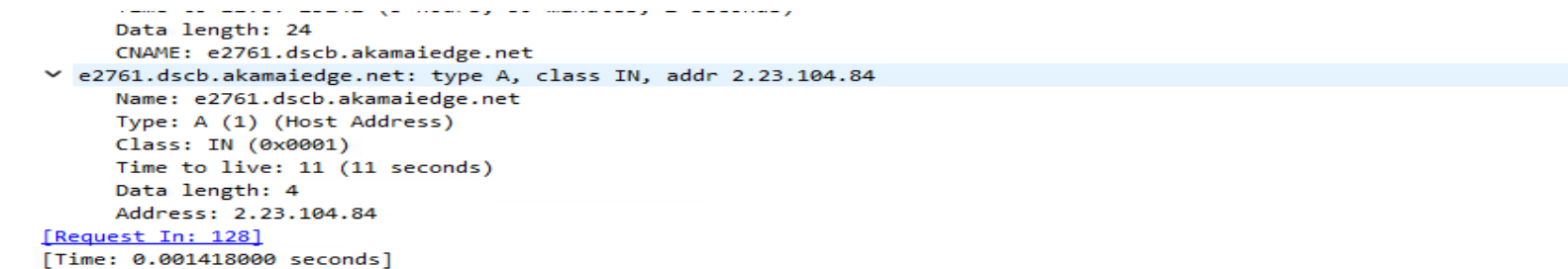
HEADERS



The screenshot shows a DNS response header in a network analysis tool. The tree view on the left indicates a 'Domain Name System (response)' packet. The main pane displays the following details:

- Transaction ID: 0x08df
- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 3
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - deepsecaas11-en.gfrbridge.trendmicro.com: type A, class IN
 - Name: deepsecaas11-en.gfrbridge.trendmicro.com
 - [Name Length: 40]
 - [Label Count: 4]
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)
- Answers
 - deepsecaas11-en.gfrbridge.trendmicro.com: type CNAME, class IN, cname wildcard-dsa2.gfrbridge.trendmicro.com.edgekey.net
 - Name: deepsecaas11-en.gfrbridge.trendmicro.com
 - Type: CNAME (5) (Canonical NAME for an alias)
 - Class: IN (0x0001)
 - Time to live: 1117 (18 minutes, 37 seconds)
 - Data length: 52
 - CNAME: wildcard-dsa2.gfrbridge.trendmicro.com.edgekey.net
 - wildcard-dsa2.gfrbridge.trendmicro.com.edgekey.net: type CNAME, class IN, cname e2761.dscb.akamaiedge.net
 - Name: wildcard-dsa2.gfrbridge.trendmicro.com.edgekey.net
 - Type: CNAME (5) (Canonical NAME for an alias)
 - Class: IN (0x0001)
 - Time to live: 13142 (3 hours, 39 minutes, 2 seconds)
 - Data length: 24

Figure 1: Header do DNS



This block continues the details of the DNS response header, showing the final answer and timing information:

- Data length: 24
- CNAME: e2761.dscb.akamaiedge.net
- e2761.dscb.akamaiedge.net: type A, class IN, addr 2.23.104.84
 - Name: e2761.dscb.akamaiedge.net
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)
 - Time to live: 11 (11 seconds)
 - Data length: 4
 - Address: 2.23.104.84
- [Request In: 128]
- [Time: 0.001418000 seconds]

Figure 2: Resto do Header do DNS

ENCAPSULAMENTO

```
> Frame 129: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: CheckPointSo_81:09:34 (00:1c:7f:81:09:34), Dst: VMware_a4:8a:8c (00:50:56:a4:8a:8c)
> Internet Protocol Version 4, Src: 10.40.48.10, Dst: 10.240.4.100
> User Datagram Protocol, Src Port: 53, Dst Port: 50515
> Domain Name System (response)
```

Figure 3: Encapsulamento do DNS

FLUXO DE MENSAGENS

Tipo	Origem	Destino
IPV4	10.40.48.10	10.240.4.100
Porta	53	50515
MAC	00:1c:7f:81:09:34	00:50:56:a4:8a:8c

HTTP

HEADERS

913	5.192737	10.240.4.100	10.250.0.78	HTTP	395	GET /Content/9E/2688A73841E78A2866D5690897CC280051637D9E.cab HTTP/1.1
914	5.193443	10.250.0.78	10.240.4.100	HTTP	187	HTTP/1.1 404 Not Found
937	5.264120	10.240.4.100	10.250.0.78	HTTP	395	GET /Content/46/34E8C362C1132AC50ACB6BCEEA4487AFC26A2846.exe HTTP/1.1
938	5.264887	10.250.0.78	10.240.4.100	HTTP	187	HTTP/1.1 404 Not Found
1871	8.944837	10.240.4.100	23.59.234.19	HTTP	905	GET /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
1909	9.079875	23.59.234.19	10.240.4.100	HTTP	274	HTTP/1.1 200 OK (text/html)

> Frame 1871: 905 bytes on wire (7240 bits), 905 bytes captured (7240 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: VMware_a4:8a:8c (00:50:56:a4:8a:8c), Dst: CheckPointSo_81:09:34 (00:1c:7f:81:09:34)
> Internet Protocol Version 4, Src: 10.240.4.100, Dst: 23.59.234.19
> Transmission Control Protocol, Src Port: 59588, Dst Port: 80, Seq: 1, Ack: 1, Len: 851
> Hypertext Transfer Protocol
 [truncated]GET /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
 [[[truncated]Expert Info (Chat/Sequence): GET /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
 [GET /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI [truncated]: /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
 User-Agent: TMUFE\r\n
 Accept: */*\r\n
 Host: dsaas.url.trendmicro.com:80\r\n
 Connection: Close\r\n
 Cache-Control: no-cache\r\n
 [truncated]X-TM-UF-INFO: 376/Uj3tcG7ArMGAK_iYi4140vrmQfYBf1-4FI3NXouIVz1ijmE7IAkvly2pksThdh1hhMDU-yGHEg472QunzD1IGXvxpwlLm7fR4NJRmU_GNrcgpFPsS3dCilj5J5KFVAIDSu4r3jlpCbfxG1ANQ6FNUB6PSU3ULYn9_E07e0sbTb1x4ec5SIXPgCim7vFKszpuEngTN6Nn4Y4yQsY\r\n
 [Full request URI [truncated]: http://dsaas.url.trendmicro.com:80/T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP request 1/1]
 [Response in frame: 1909]

Figure 4: Header do GET

✓	[truncated]GET /T/320/WbXPz4XXxrXsvj68JVO_ZZyC9rI4K_OGpe46YoZxqrRCDxc9eQnJrndcgY4XDNc6Y-001A90p1j4soQqCgCZXu_5wII8uL6g60N4mxz3cRKBDJ2Rt_J5egCto_EPUNzveFmA0IS61HEy0u70moB1UqmcXZgVbhoZdTvosQsyVr_XPHPnTcZjHsaNTNpcA4Z0JATas0va1Ha73TjBhidj8YE20I1pz3f HTTP/1.1
✓	Hypertext Transfer Protocol
✓	HTTP/1.1 200 OK\r\n
✓	[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
	[HTTP/1.1 200 OK\r\n]
	[Severity level: Chat]
	[Group: Sequence]
	Response Version: HTTP/1.1
	Status Code: 200
	[Status Code Description: OK]
	Response Phrase: OK
	Content-Type: text/html\r\n
	Last-Modified: Sun, 01 Sep 2024 19:51:29 GMT\r\n
	Server: Trend Micro 2.5\r\n
	X-Frame-Options: DENY\r\n
✓	Content-Length: 220\r\n
	[Content length: 220]
	Expires: Sun, 01 Sep 2024 19:51:30 GMT\r\n
	Cache-Control: max-age=0, no-cache, no-store\r\n
	Pragma: no-cache\r\n
	Date: Sun, 01 Sep 2024 19:51:30 GMT\r\n
	Connection: close\r\n
	\r\n
	[HTTP response 1/1]
	[Time since request: 0.135038000 seconds]

Figure 5: Header da Resposta

ENCAPSULAMENTO

```
> Frame 1871: 905 bytes on wire (7240 bits), 905 bytes captured (7240 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: VMware_a4:8a:8c (00:50:56:a4:8a:8c), Dst: CheckPointSo_81:09:34 (00:1c:7f:81:09:34)
> Internet Protocol Version 4, Src: 10.240.4.100, Dst: 23.59.234.19
> Transmission Control Protocol, Src Port: 59588, Dst Port: 80, Seq: 1, Ack: 1, Len: 851
> Hypertext Transfer Protocol
```

Figure 6: Encapsulamento do GET

```
> Frame 1909: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: CheckPointSo_81:09:34 (00:1c:7f:81:09:34), Dst: VMware_a4:8a:8c (00:50:56:a4:8a:8c)
> Internet Protocol Version 4, Src: 23.59.234.19, Dst: 10.240.4.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 59588, Seq: 320, Ack: 852, Len: 220
> [2 Reassembled TCP Segments (539 bytes): #1908(319), #1909(220)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (1 lines)
```

Figure 7: Encapsulamento da Resposta

FLUXO DE MENSAGENS

Tipo	Origem	Destino
IPV4	23.59.234.19	10.240.4.100
Porta	80	59588
MAC	00:1c:7f:81:09:34	00:50:56:a4:8a:8c

HTTPS

HEADERS

```
Transport Layer Security
  TLV1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 9384
    Encrypted Application Data [truncated]: 107210f007ca599eb0d1fd33c70e8d13ff722e15a963afbf14d0c9dcbe4ca00598872b3ed1a0a9b8c4f0e2a719e219b82f381606612
```

Figure 9: Header do HTTPS

```
Transport Layer Security
  TLV1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 34
    Encrypted Application Data: 9c6d4f1139263ee7977f098f3145bdee910f2aefd877e06667441c8539122dd36b37
```

Figure 8: Header da Primeira Resposta do HTTPS

```
Transport Layer Security
  TLV1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 34
    Encrypted Application Data: 9c6d4f1139263ee8d10210b016f0863fe0a5a3984159831a94a3bc00c33c24743a4c
  TLV1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 34
    Encrypted Application Data: 9c6d4f1139263ee9bc0b25380f6f876cbfd99e0b93cd06a27e00402c8e0a3aafadd9
  TLV1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 38
    Encrypted Application Data: 9c6d4f1139263eeaf140a217e1f843972141c69dbfb841c0c07358957dc24702acce164e4098
```

Figure 10: Header da Segunda Resposta do HTTPS

ENCAPSULAMENTO

```
> Frame 4: 9443 bytes on wire (75544 bits), 9443 bytes captured (75544 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: VMware_a4:8a:8c (00:50:56:a4:8a:8c), Dst: CheckPointSo_81:09:34 (00:1c:7f:81:09:34)
> Internet Protocol Version 4, Src: 10.240.4.100, Dst: 10.40.39.209
> Transmission Control Protocol, Src Port: 22443, Dst Port: 26540, Seq: 303, Ack: 1, Len: 9389
> Transport Layer Security
```

Figure 11: Encapsulamento da Requisição do HTTPS

```

> Frame 5: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: CheckPointSo_81:09:34 (00:1c:7f:81:09:34), Dst: VMware_a4:8a:8c (00:50:56:a4:8a:8c)
> Internet Protocol Version 4, Src: 10.40.39.209, Dst: 10.240.4.100
> Transmission Control Protocol, Src Port: 26540, Dst Port: 22443, Seq: 1, Ack: 303, Len: 39
> Transport Layer Security

```

Figure 13: Encapsulamento da Primeira Resposta do HTTPS

```

> Frame 6: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface \Device\NPF_{FB59989A-1BAE-408F-BE71-E52D3F6C1F92}, id 0
> Ethernet II, Src: CheckPointSo_81:09:34 (00:1c:7f:81:09:34), Dst: VMware_a4:8a:8c (00:50:56:a4:8a:8c)
> Internet Protocol Version 4, Src: 10.40.39.209, Dst: 10.240.4.100
> Transmission Control Protocol, Src Port: 26540, Dst Port: 22443, Seq: 40, Ack: 303, Len: 121
> Transport Layer Security

```

Figure 12: Encapsulamento da Segunda Resposta do HTTPS

FLUXO DE MENSAGENS DO HTTPS

Tipo	Origem	Destino
IPV4	10.240.4.100	10.40.39.289
Porta	22443	26540
MAC	00:50:56:A4:8A:8C	00:1c:7f:81:09:34

FLUXO DE MENSAGENS DA PRIMEIRA RESPOSTA DO HTTPS

Tipo	Origem	Destino
IPV4	10.40.39.209	10.240.4.100
Porta	26540	22443
MAC	00:1c:7f:81:09:34	00:50:56:a4:8a:8c

FLUXO DE MENSAGENS DA SEGUNDA RESPOSTA DO HTTPS

Tipo	Origem	Destino
IPV4	10.40.39.209	10.240.4.100
Porta	26540	22443
MAC	00:1c:7f:81:09:34	00:50:56:a4:8a:8c

DHCP

HEADERS

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xeea34642

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address:

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: VMware_a4:b8:35 (00:50:56:a4:b8:35)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)

- Length: 1
- DHCP: Discover (1)

Option: (61) Client identifier

- Length: 7
- Hardware type: Ethernet (0x01)
- Client MAC address: VMware_a4:b8:35 (00:50:56:a4:b8:35)

Option: (12) Host Name

- Length: 15
- Host Name: PUCRSVDIEPINF49

Option: (60) Vendor class identifier

- Length: 8
- Vendor class identifier: MSFT 5.0

Option: (55) Parameter Request List

- Length: 14
- Parameter Request List Item: (1) Subnet Mask
- Parameter Request List Item: (3) Router
- Parameter Request List Item: (6) Domain Name Server
- Parameter Request List Item: (15) Domain Name
- Parameter Request List Item: (31) Perform Router Discovery
- Parameter Request List Item: (33) Static Route
- Parameter Request List Item: (43) Vendor-Specific Information
- Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
- Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
- Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
- Parameter Request List Item: (119) Domain Search
- Parameter Request List Item: (121) Classless Static Route
- Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
- Parameter Request List Item: (252) Private/Proxy Autodiscovery

Option: (255) End

- Option End: 255

Padding: 00000000

Criptografia: Não (Plain Text)

ENCAPSULAMENTO

Ethernet II, Src: VMware_a4:b8:35, Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

FLUXO DE MENSAGENS

Tipo	Origem	Destino
IPV4	0.0.0.0	255.255.255.255
Porta	68	67
MAC	00:50:56:a4:b8:35	ff:ff:ff:ff:ff:ff