WHAT HAPPENED TO NALC?

CREATING THE NEXT®

What you were provided

- Web root was encrypted and a phone call reported it was cryptolockered
- You are provided by the initial response team the web root and the web logs

- All times given in UTC.

Attack timeline

- 10/27 – sent mail
- 10/29 17:38 – Bob opened mail

- The mail contained an Excel spreadsheet with a macro that downloaded a secondary payload and opened a backdoor running on an outbound https tunnel to store.cloudxlarge.com.
- At the time the project started this spreadsheet would bypass fully updated Windows Defender on Windows 10. It could not escalate to System on Windows 10, but that ended up not mattering because I didn’t need System, and Bob’s workstation was 2003.
- This tunnel was encrypted with a Let’s Encrypt cert, which makes it harder to find.

Post Exploitation

- 17:39 – Got System level access, dumped hashes from memory and installed a keylogger
- 17:40 – set Registry key to restart payload when Bob logs in
- 17:43 – ran port scan of entire environment
- 18:11 – Bob logs in to web serverr

Lateral movement

- 18:22 -- used Bob’s password from web site to ssh to web server, which succeeds
- 18:23 -- used sudo for the first time, which also succeeds
- 18:35 – installed a backdoor on webserver

Georgia Tech

SAMPLE INVESTIGATION

CREATING THE NEXT®

What is our first time for a search?

```
tulkas:277% TZ=UTC ls -l var/www/html
total 352
-rw-------    1 chris  staff    418 Oct 29 19:32 index.php
-rw-------    1 chris  staff  19935 Oct 29 19:32 license.txt
-rw-------    1 chris  staff   7413 Oct 29 19:32 readme.html
-rw-------    1 chris  staff    724 Oct 29 19:32 upload.php
drwx------    3 chris  staff    102 Oct 29 19:20 uploads
-rw-------    1 chris  staff   5447 Oct 29 19:32 wp-activate.php
drwx------   89 chris  staff   3026 Sep 19 21:21 wp-admin
-rw-------    1 chris  staff    364 Oct 29 19:32 wp-blog-header.php
-rw-------    1 chris  staff   1627 Oct 29 19:32 wp-comments-post.php
-rw-------    1 chris  staff   2853 Oct 29 19:32 wp-config-sample.php
```

File encryption was performed at 19:32 UTC.

What timezone is the system?

```
tulkas:285% TZ=UTC ls -l var/log/syslog
-rw-------  1 chris  staff  10082 Oct 30 12:09 var/log/syslog
tulkas:286% tail -1 var/log/syslog
Oct 30 12:09:01 ip-10-0-0-14 CRON[10967]: (root) CMD (   [ -x /u
tulkas:287%
```

System logs are UTC. You could also have gotten this from /etc/timezone if you got a dump of the filesystem, or asked the sysadmins

What else happened around 19:32?

```
Oct 29 18:42:46 ip-10-0-0-14 sshd[7223]: Accepted password for bob from 10.0.3.15 port 4465 ssh2
Oct 29 18:42:46 ip-10-0-0-14 sshd[7223]: pam_unix(sshd:session): session opened for user bob by (uid=0)
Oct 29 18:42:46 ip-10-0-0-14 systemd-logind[1362]: New session 88 of user bob.
Oct 29 18:42:50 ip-10-0-0-14 sshd[7223]: pam_unix(sshd:session): session closed for user bob
Oct 29 18:42:50 ip-10-0-0-14 systemd-logind[1362]: Removed session 88.
Oct 29 18:44:48 ip-10-0-0-14 sshd[7264]: Accepted password for bob from 10.0.3.15 port 4560 ssh2
Oct 29 18:44:48 ip-10-0-0-14 sshd[7264]: pam_unix(sshd:session): session opened for user bob by (uid=0)
Oct 29 18:44:48 ip-10-0-0-14 systemd-logind[1362]: New session 89 of user bob.
Oct 29 18:44:52 ip-10-0-0-14 sshd[7264]: pam_unix(sshd:session): session closed for user bob
Oct 29 18:44:52 ip-10-0-0-14 systemd-logind[1362]: Removed session 89.
Oct 29 19:08:26 ip-10-0-0-14 sshd[7340]: Accepted password for bob from 10.0.3.15 port 4863 ssh2
Oct 29 19:08:26 ip-10-0-0-14 sshd[7340]: pam_unix(sshd:session): session opened for user bob by (uid=0)
Oct 29 19:08:26 ip-10-0-0-14 systemd-logind[1362]: New session 90 of user bob.
Oct 29 19:08:31 ip-10-0-0-14 sudo:      bob : unable to resolve host ip-10-0-0-14
Oct 29 19:09:01 ip-10-0-0-14 CRON[7377]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 29 19:09:01 ip-10-0-0-14 CRON[7377]: pam_unix(cron:session): session closed for user root
Oct 29 19:09:23 ip-10-0-0-14 sudo:      bob : TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
Oct 29 19:09:23 ip-10-0-0-14 sudo: pam_unix(sudo:session): session opened for user root by bob(uid=0)
Oct 29 19:17:01 ip-10-0-0-14 CRON[7431]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 29 19:17:01 ip-10-0-0-14 CRON[7431]: pam_unix(cron:session): session closed for user root
Oct 29 19:19:46 ip-10-0-0-14 sudo:   ubuntu : unable to resolve host ip-10-0-0-14
Oct 29 19:19:46 ip-10-0-0-14 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/ufw status v
Oct 29 19:19:46 ip-10-0-0-14 sudo: pam_unix(sudo:session): session opened for user root by ubuntu(uid=0)
Oct 29 19:19:46 ip-10-0-0-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 29 19:33:32 ip-10-0-0-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 29 19:34:53 ip-10-0-0-14 sshd[7340]: pam_unix(sshd:session): session closed for user bob
Oct 29 19:39:01 ip-10-0-0-14 CRON[8064]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 29 19:39:01 ip-10-0-0-14 CRON[8064]: pam_unix(cron:session): session closed for user root
Oct 29 19:44:59 ip-10-0-0-14 sshd[6857]: pam_unix(sshd:session): session closed for user bob
Oct 29 19:44:59 ip-10-0-0-14 sudo: pam_unix(sudo:session): session closed for user root
```

{"username": "-", "store_number": 1, "hostname": "WS7-2003-BOB", "display_name": "TSK:/Documents and Settings/bob/Desktop/N
ALC-salaries.xls", "uuid": "fd46c2e07bdc46c98f9dd2470d8fad4e", "timestamp_desc": "crtime", "timestamp": 1509298675951541, "
parser": "filestat", "filename": "/Documents and Settings/bob/Desktop/NALC-salaries.xls", "data_type": "fs:stat", "store_in
dex": 469194, "tag": null, "offset": 0, "pathspec": "{\"type_indicator\": \"TSK\", \"inode\": 60847, \"location\": \"/Docum
ents and Settings/bob/Desktop/NALC-salaries.xls\", \"parent\": \"{\\\"parent\\\": \\\"{\\\\\\\"type_indicator\\\\\\\": \\\\
\\\"OS\\\\\\\", \\\\\\\"location\\\\\\\": \\\\\\\"/mnt/hgfs/Disk Images/bob_workstation\\\\\\\"}\\\", \\\"type_indicator\\\\
": \\\"TSK_PARTITION\\\", \\\"part_index\\\": 2, \\\"location\\\": \\\"/p1\\\", \\\"start_offset\\\": 1048576}\"}", "alloca
ted": true, "fs_type": "NTFS_DETECT", "inode": 60847, "size": [44544]}

This timestamp is 2017/10/29 at 17:37:55

```
From ubuntu@cloudxlarge.com  Fri Oct 27 01:14:31 2017
Return-Path: <ubuntu@cloudxlarge.com>
X-Original-To: bob@northamericanlumbercoalition.com
Delivered-To: bob@northamericanlumbercoalition.com
Received: from ip-10-0-80-181.ec2.internal (ec2-52-1-52-89.compute-1.amazonaws.com [52.1.52.89])
        by mail.northamericanlumbercoalition.com (Postfix) with ESMTP id EA3C161258
        for <bob@northamericanlumbercoalition.com>; Fri, 27 Oct 2017 01:14:30 +0000 (UTC)
Received: by ip-10-0-80-181.ec2.internal (Postfix, from userid 1000)
        id 58AC8465D9; Thu, 26 Oct 2017 16:17:55 +0000 (UTC)
Content-Type: multipart/mixed; boundary="1535362749-1509034109=:26173"
MIME-Version: 1.0
To: "Joe Chandler" <joe@northamericanlumbercoalition.com>
Subject: Proposed salary structure
X-Mailer: mail (GNU Mailutils 2.99.99)
Message-Id: <20171026160829.5F311465D4@northamericanlumbercoalition.com>
Date: Thu, 26 Oct 2017 16:08:29 +0000 (UTC)
From: "Annie Smith" <annie@northamericanlumbercoalition.com>
X-UID: 8
Content-Length: 47478
Status: RO
X-Status: A

--1535362749-1509034109=:26173
Content-ID: <20171026160829.26173@ip-10-0-80-181.ec2.internal>
Content-Type: text/plain

Please see the attached proposal.

--1535362749-1509034109=:26173
Content-ID: <20171026160829.26173.1@ip-10-0-80-181.ec2.internal>
Content-Type: application/octet-stream; name=NALC-salaries.xls
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=NALC-salaries.xls

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAABAAAAAQAAAAAAAAAA
```

33 / 59

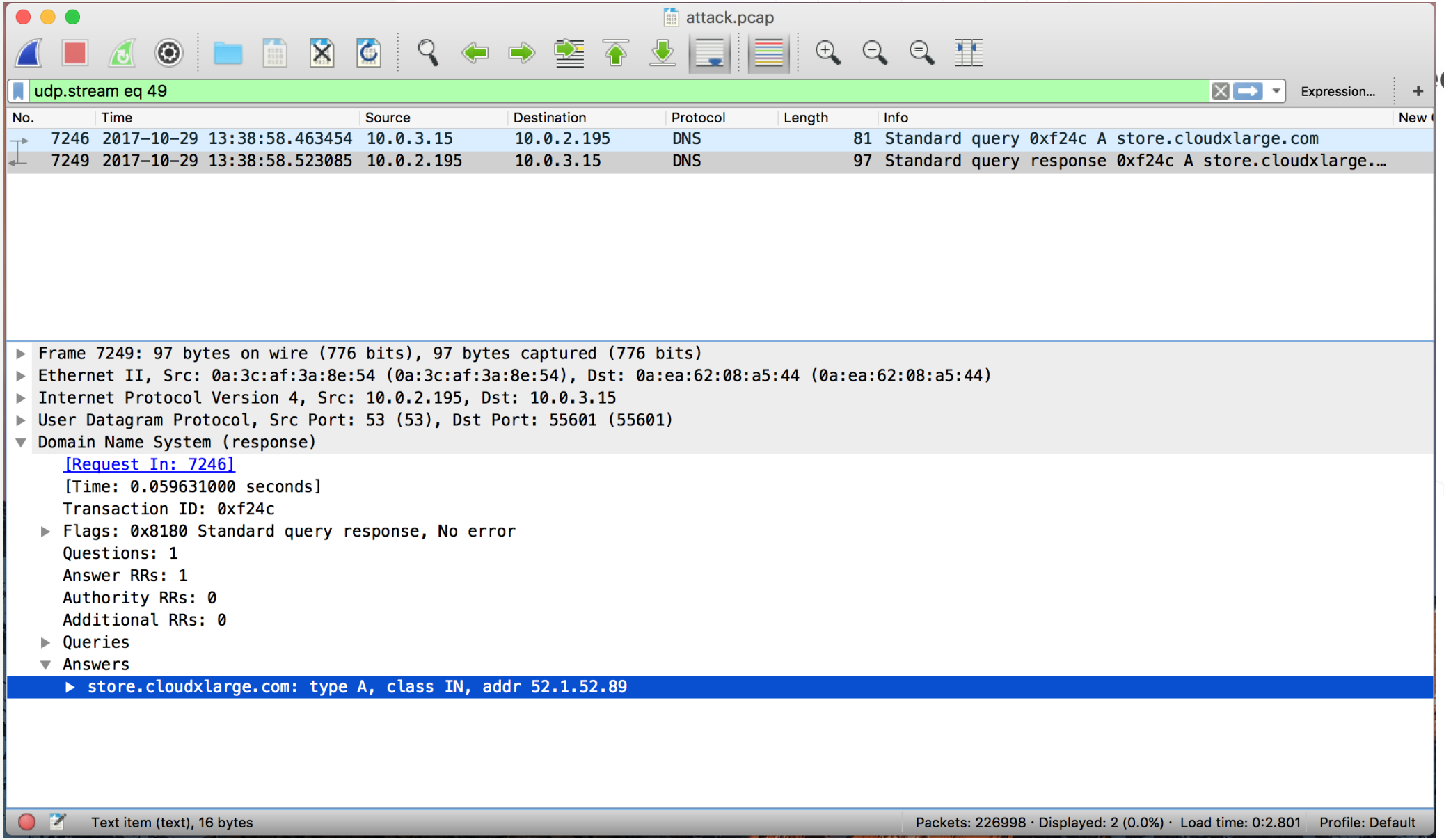
33 engines detected this file

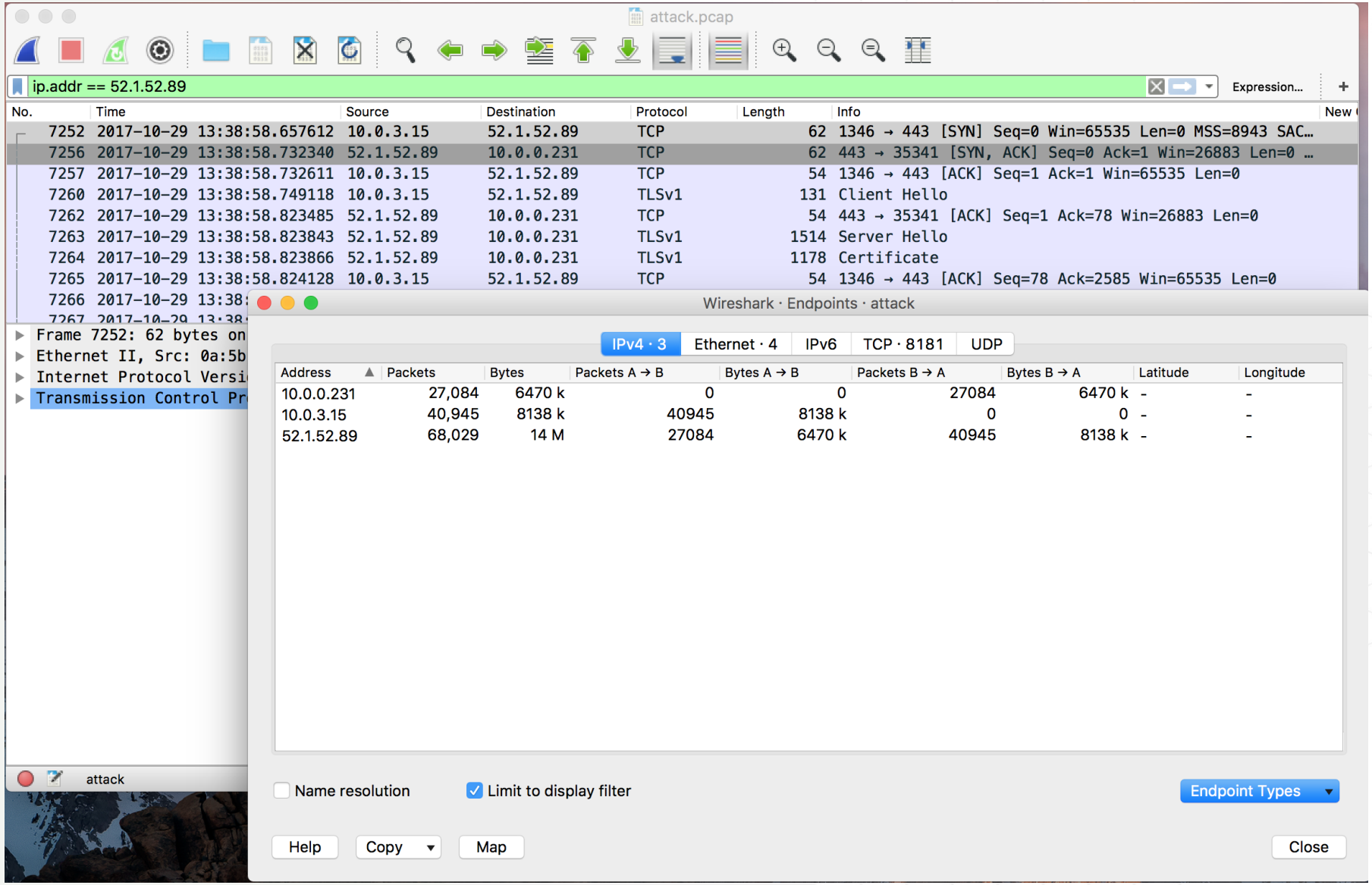
SHA-256	a8e51422afb18777d892ce0fceb15bc08df6f6e265b66b5ccab8021e53fafb97
File name	localfile~
File size	43.5 KB
Last analysis	2017-11-13 16:40:51 UTC

Detection | Details | Relations | Community 2

Ad-Aware	VB.Downloader.1.Gen	AegisLab	Troj.Script.Agent!c
ALYac	VB.Downloader.1.Gen	Antiy-AVL	Trojan/Script.Agent.gen
Arcabit	HEUR.VBA.Trojan.e	Avast	VBA:Downloader-BUB [Trj]
AVG	VBA:Downloader-BUB [Trj]	Avira	HEUR/Macro.Agent
AVware	LooksLike.Macro.Malware.c (v)	BitDefender	VB.Downloader.1.Gen
ClamAV	Doc.Macro.Obfuscation-6360615-0	Cyren	Trojan.NPGI-7
DrWeb	modification of W97M.Suspicious.1	Emsisoft	VB.Downloader.1.Gen (B)
eScan	VB.Downloader.1.Gen	ESET-NOD32	VBA/Obfuscated.P
F-Secure	VB.Downloader.1.Gen	Fortinet	VBA/Agent.DEM!tr.dldr
GData	VB.Downloader.1.Gen	Ikarus	Trojan.VBA.Obfuscated
Kaspersky	HEUR:Trojan.Script.Agent.gen	MAX	malware (ai score=100)
McAfee	RDN/Generic Downloader.x	McAfee-GW-Edition	RDN/Generic Downloader.x
Microsoft	Trojan:Win32/Skeeyah.A!rfn	NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzi
Qihoo-360	heur.macro.powershell.x	Rising	Macro.Agent.cg (CLASSIC)

Georgia Tech


attack.pcap
udp.stream eq 49
Expression...
No. Time Source Destination Protocol Length Info
7246 2017-10-29 13:38:58.463454 10.0.3.15 10.0.2.195 DNS 81 Standard query 0xf24c A store.cloudxlarge.com
7249 2017-10-29 13:38:58.523085 10.0.2.195 10.0.3.15 DNS 97 Standard query response 0xf24c A store.cloudxlarge.…
Frame 7249: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
Ethernet II, Src: 0a:3c:af:3a:8e:54 (0a:3c:af:3a:8e:54), Dst: 0a:ea:62:08:a5:44 (0a:ea:62:08:a5:44)
Internet Protocol Version 4, Src: 10.0.2.195, Dst: 10.0.3.15
User Datagram Protocol, Src Port: 53 (53), Dst Port: 55601 (55601)
Domain Name System (response)
[Request In: 7246]
[Time: 0.059631000 seconds]
Transaction ID: 0xf24c
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
store.cloudxlarge.com: type A, class IN, addr 52.1.52.89
Text item (text), 16 bytes
Packets: 226998 · Displayed: 2 (0.0%) · Load time: 0:2.801
Profile: Default



Georgia Tech

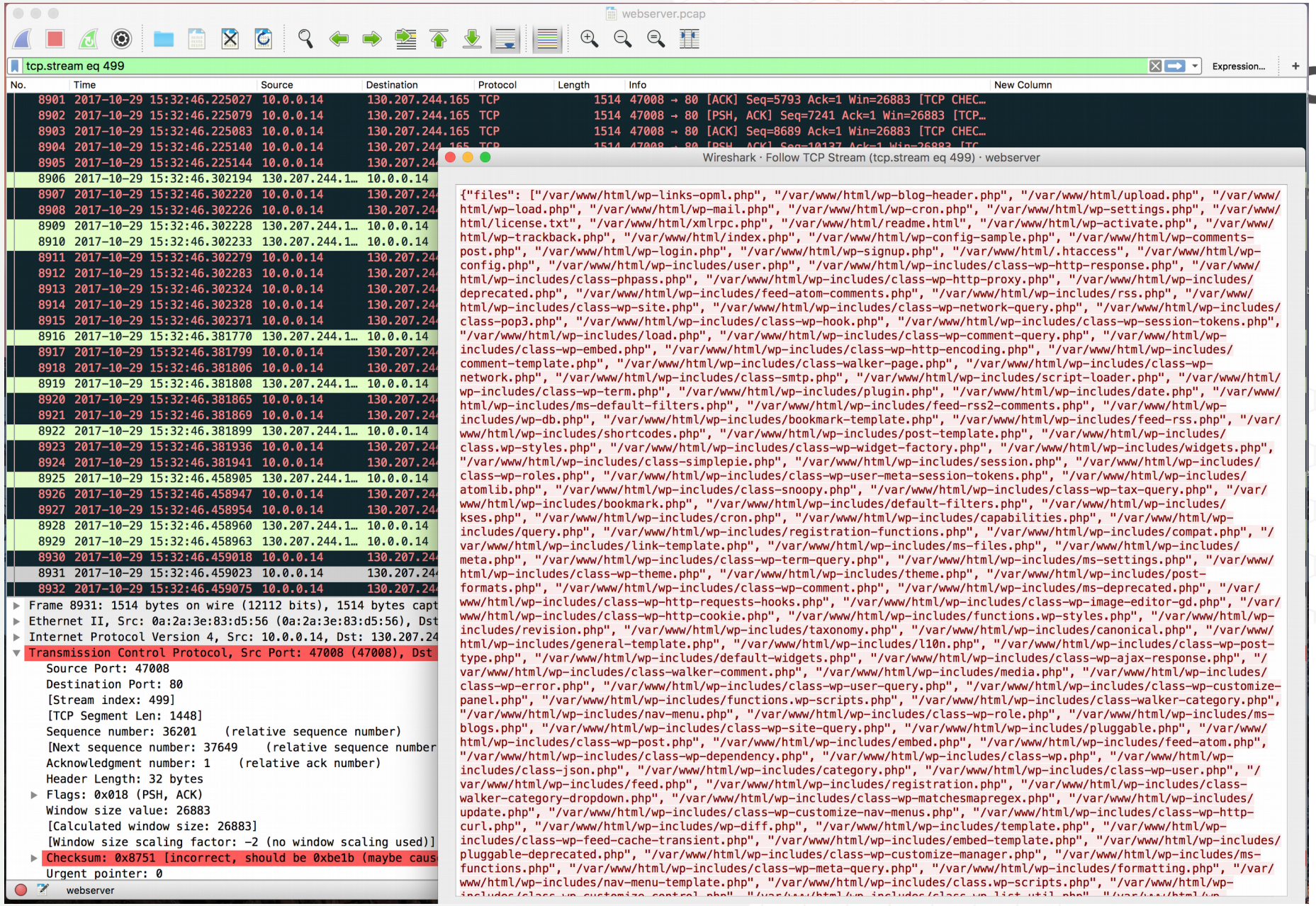
CREATING THE NEXT®

chris@tulkas:~/t — less var/log/apt/history.log — 134×43

```
Start-Date: 2017-10-27  18:22:58
Commandline: apt install traceroute
Requested-By: ubuntu (1000)
Install: traceroute:amd64 (1:2.0.21-1)
End-Date: 2017-10-27  18:22:59

Start-Date: 2017-10-28  06:10:24
Commandline: /usr/bin/unattended-upgrade
Upgrade: wget:amd64 (1.17.1-1ubuntu1.2, 1.17.1-1ubuntu1.3)
End-Date: 2017-10-28  06:10:25

Start-Date: 2017-10-28  17:50:29
Commandline: apt full-upgrade
Requested-By: ubuntu (1000)
Upgrade: libgnutls-openssl27:amd64 (3.4.10-4ubuntu1.3, 3.4.10-4ubuntu1.4), libsystemd0:amd64 (229-4ubuntu19, 229-4ubuntu21), grub-comm
on:amd64 (2.02~beta2-36ubuntu3.12, 2.02~beta2-36ubuntu3.14), grub2-common:amd64 (2.02~beta2-36ubuntu3.12, 2.02~beta2-36ubuntu3.14), ud
ev:amd64 (229-4ubuntu19, 229-4ubuntu21), grub-pc:amd
64 (2.02~beta2-36ubuntu3.12, 2.02~beta2-36ubuntu3.14), libudev1:amd64 (229-4ubuntu19, 229-4ubuntu21), grub-pc-bin:amd64 (2.02~beta2-36
ubuntu3.12, 2.02~beta2-36ubuntu3.14), systemd-sysv:amd64 (229-4ubuntu19, 229-4ubuntu21), libpam-systemd:amd64 (229-4ubuntu19, 229-4ubu
ntu21), distro-info-data:amd64 (0.28ubuntu0.3, 0.28ubuntu0.5), systemd:amd64 (229-4ubuntu19, 229-4ubuntu21), libgnutls30:amd64 (3.4.10
-4ubuntu1.3, 3.4.10-4ubuntu1.4)
End-Date: 2017-10-28  17:50:42

Start-Date: 2017-10-29  18:34:49
Commandline: apt install netcat-traditional
Requested-By: bob (1002)
Install: netcat-traditional:amd64 (1.10-41)
End-Date: 2017-10-29  18:34:50

Start-Date: 2017-10-29  19:32:00
Commandline: apt install python-minimal
Requested-By: bob (1002)
Install: python2.7-minimal:amd64 (2.7.12-1ubuntu0~16.04.1, automatic), python2.7:amd64 (2.7.12-1ubuntu0~16.04.1, automatic), python:am
d64 (2.7.11-1, automatic), libpython-stdlib:amd64 (2.7.11-1, automatic), libpython2.7-minimal:amd64 (2.7.12-1ubuntu0~16.04.1, automati
c), libpython2.7-stdlib:amd64 (2.7.12-1ubuntu0~16.04.1, automatic), python-minimal:amd64 (2.7.11-1)
End-Date: 2017-10-29  19:32:03
~
~
~
~
~
(END)
```

Georgia Tech

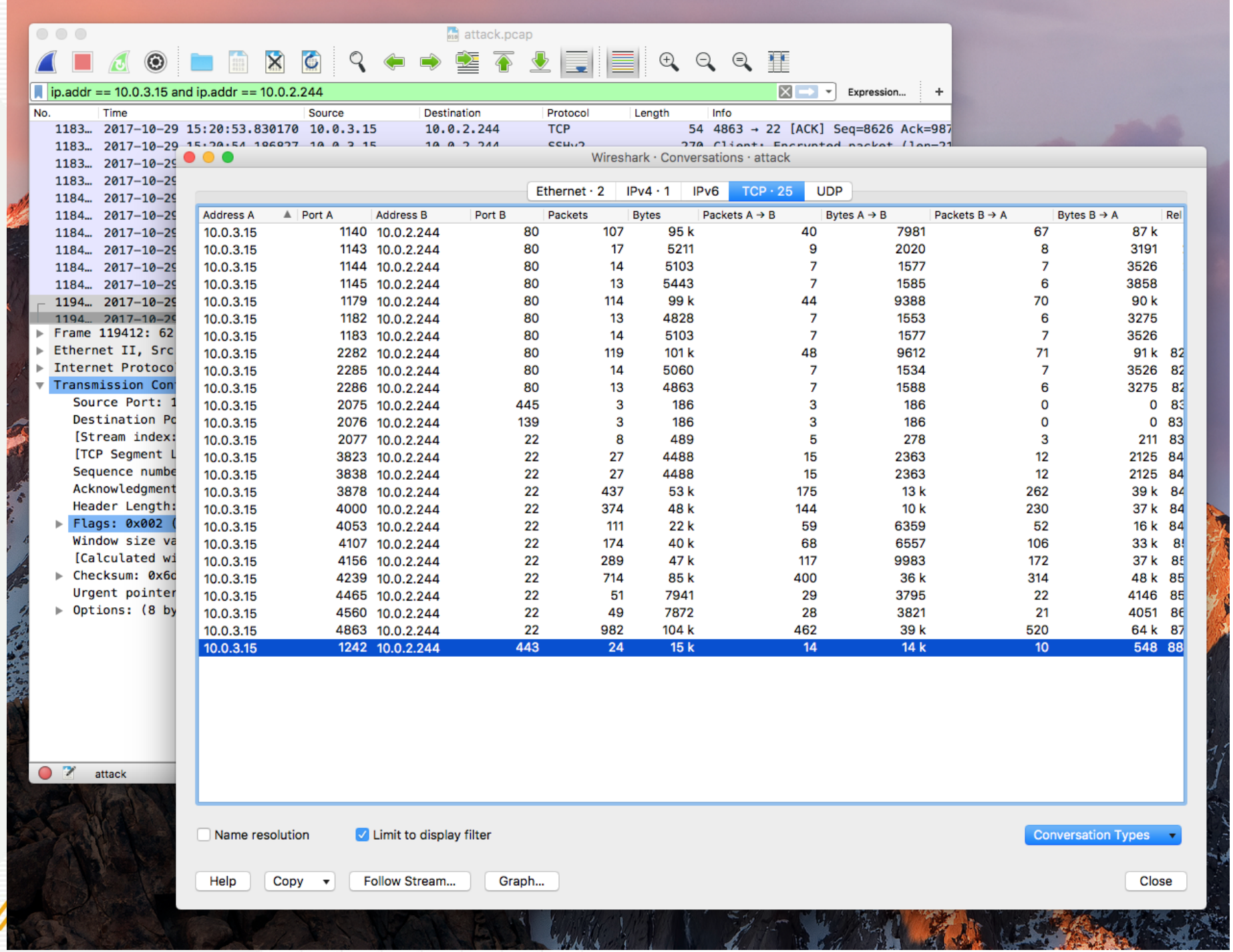
CREATING THE NEXT®

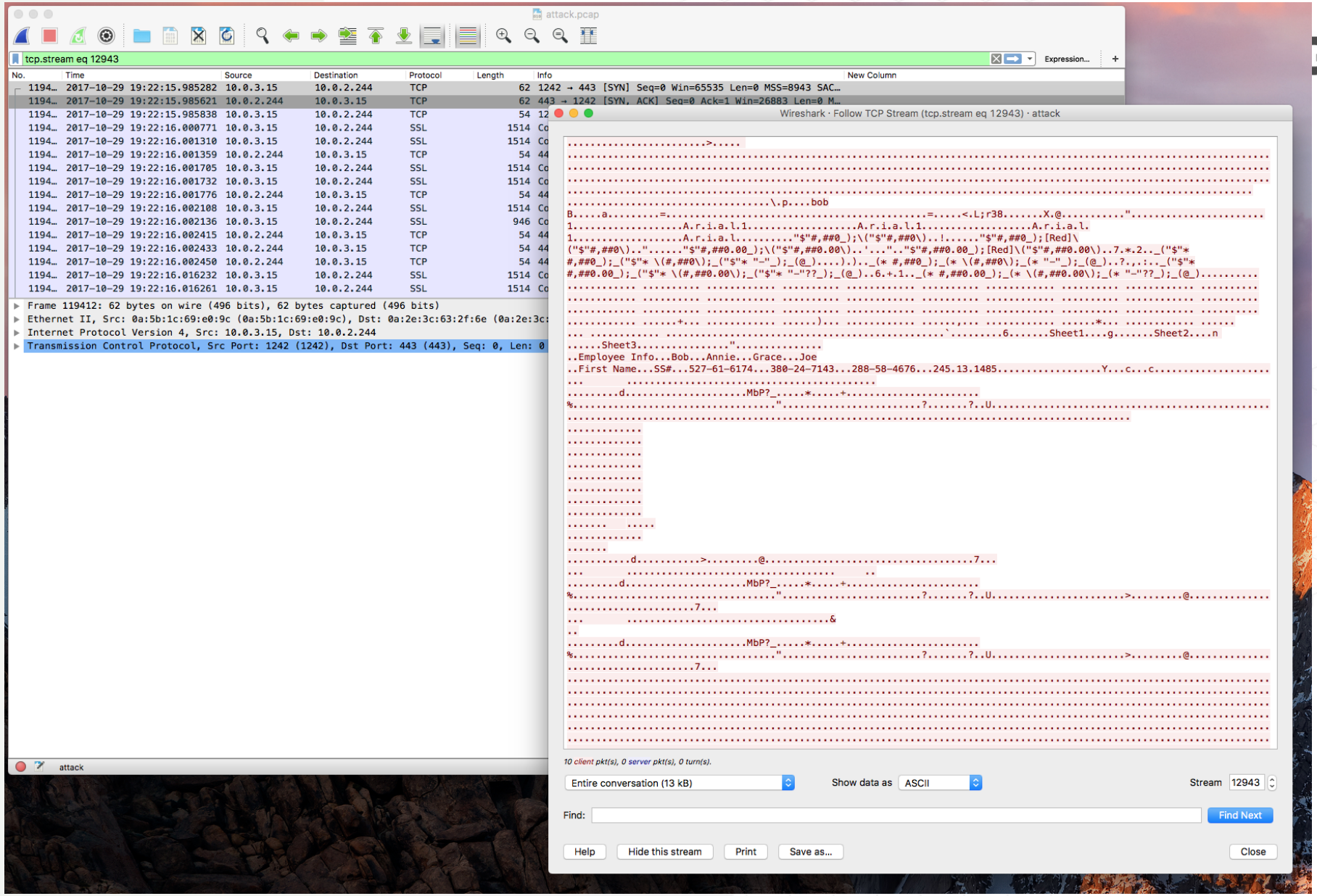


Georgia Tech

CREATING THE NEXT®

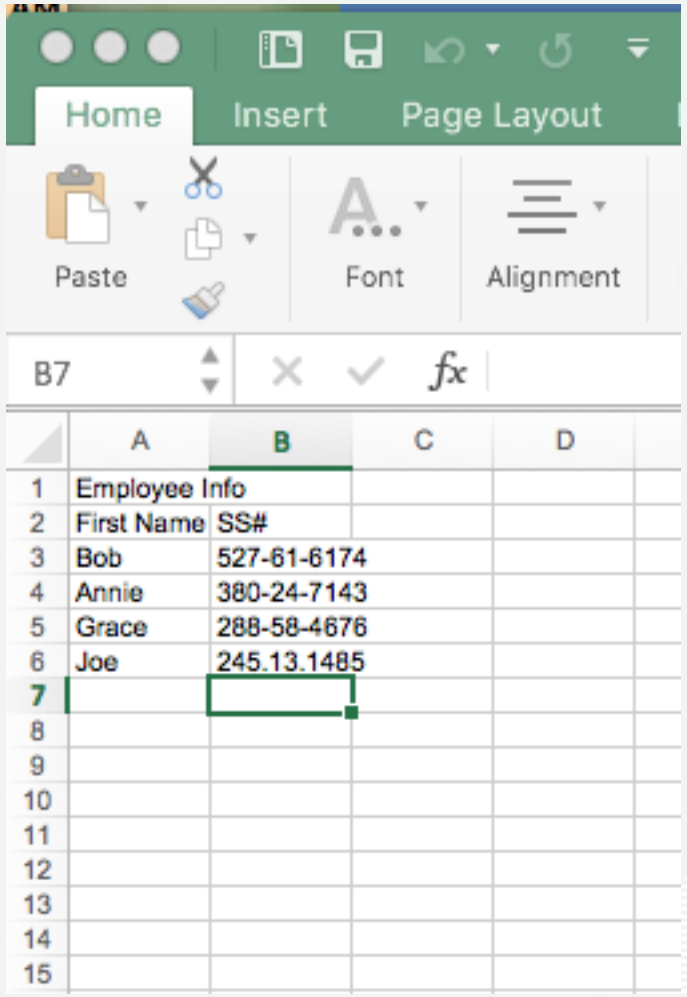
Packaging


attack.pcap
ip.addr == 10.0.3.15 and ip.addr == 10.0.2.244
Expression...
No. Time Source Destination Protocol Length Info
1183… 2017-10-29 15:20:53.830170 10.0.3.15 10.0.2.244 TCP 54 4863 → 22 [ACK] Seq=8626 Ack=987
Frame 119412: 62
Ethernet II, Src
Internet Protoco
Transmission Con
Source Port: 1
Destination Po
[Stream index:
[TCP Segment L
Sequence numbe
Acknowledgment
Header Length:
Flags: 0x002 (
Window size va
[Calculated wi
Checksum: 0x6c
Urgent pointer
Options: (8 by
attack
Wireshark · Conversations · attack
Ethernet · 2
IPv4 · 1
IPv6
TCP · 25
UDP
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel
10.0.3.15 1140 10.0.2.244 80 107 95 k 40 7981 67 87 k
10.0.3.15 1143 10.0.2.244 80 17 5211 9 2020 8 3191
10.0.3.15 1144 10.0.2.244 80 14 5103 7 1577 7 3526
10.0.3.15 1145 10.0.2.244 80 13 5443 7 1585 6 3858
10.0.3.15 1179 10.0.2.244 80 114 99 k 44 9388 70 90 k
10.0.3.15 1182 10.0.2.244 80 13 4828 7 1553 6 3275
10.0.3.15 1183 10.0.2.244 80 14 5103 7 1577 7 3526
10.0.3.15 2282 10.0.2.244 80 119 101 k 48 9612 71 91 k 82
10.0.3.15 2285 10.0.2.244 80 14 5060 7 1534 7 3526 82
10.0.3.15 2286 10.0.2.244 80 13 4863 7 1588 6 3275 82
10.0.3.15 2075 10.0.2.244 445 3 186 3 186 0 0 83
10.0.3.15 2076 10.0.2.244 139 3 186 3 186 0 0 83
10.0.3.15 2077 10.0.2.244 22 8 489 5 278 3 211 83
10.0.3.15 3823 10.0.2.244 22 27 4488 15 2363 12 2125 84
10.0.3.15 3838 10.0.2.244 22 27 4488 15 2363 12 2125 84
10.0.3.15 3878 10.0.2.244 22 437 53 k 175 13 k 262 39 k 84
10.0.3.15 4000 10.0.2.244 22 374 48 k 144 10 k 230 37 k 84
10.0.3.15 4053 10.0.2.244 22 111 22 k 59 6359 52 16 k 84
10.0.3.15 4107 10.0.2.244 22 174 40 k 68 6557 106 33 k 85
10.0.3.15 4156 10.0.2.244 22 289 47 k 117 9983 172 37 k 85
10.0.3.15 4239 10.0.2.244 22 714 85 k 400 36 k 314 48 k 85
10.0.3.15 4465 10.0.2.244 22 51 7941 29 3795 22 4146 85
10.0.3.15 4560 10.0.2.244 22 49 7872 28 3821 21 4051 86
10.0.3.15 4863 10.0.2.244 22 982 104 k 462 39 k 520 64 k 87
10.0.3.15 1242 10.0.2.244 443 24 15 k 14 14 k 10 548 88
Name resolution
Limit to display filter
Conversation Types
Help
Copy
Follow Stream...
Graph...
Close



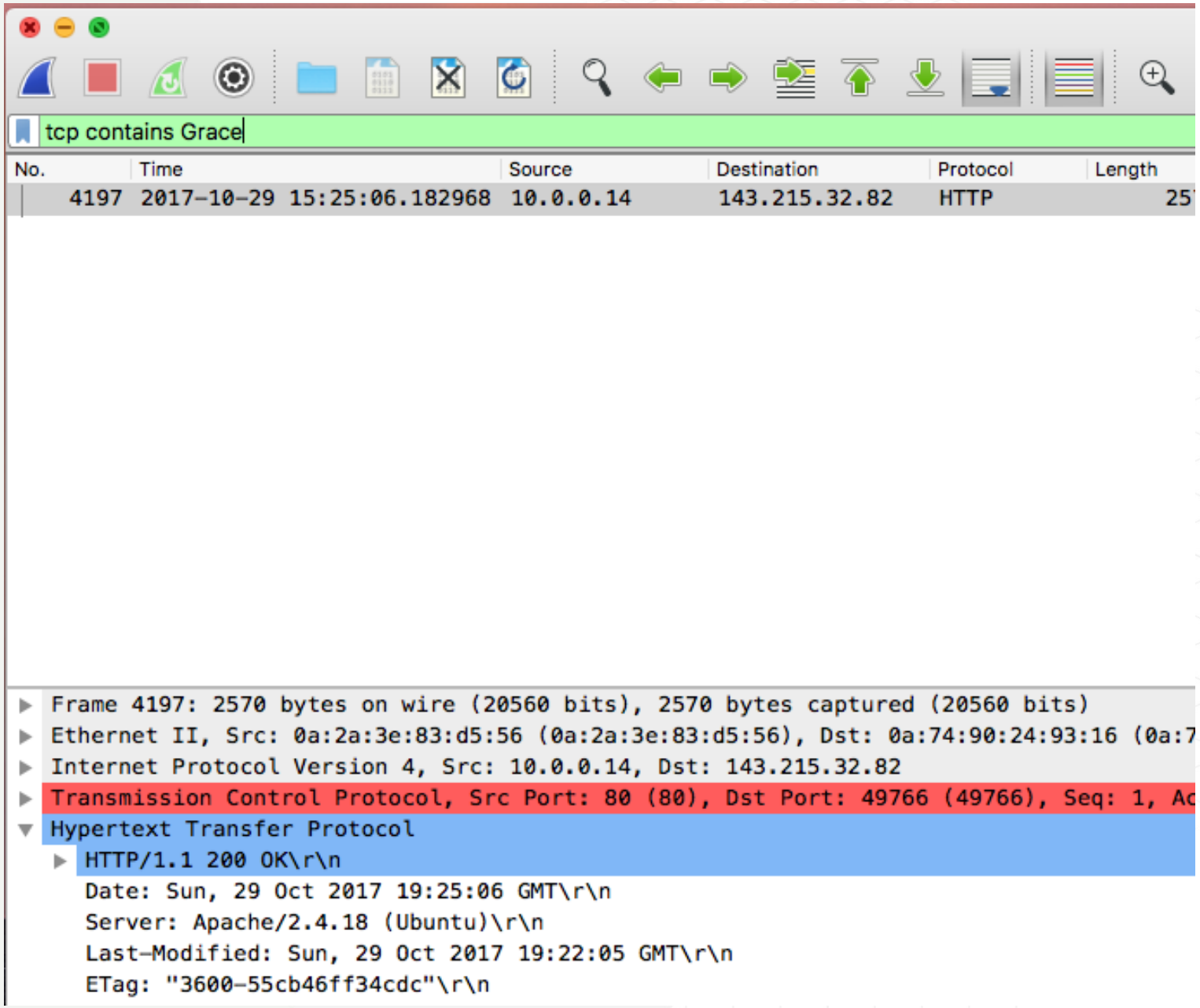
Georgia Tech

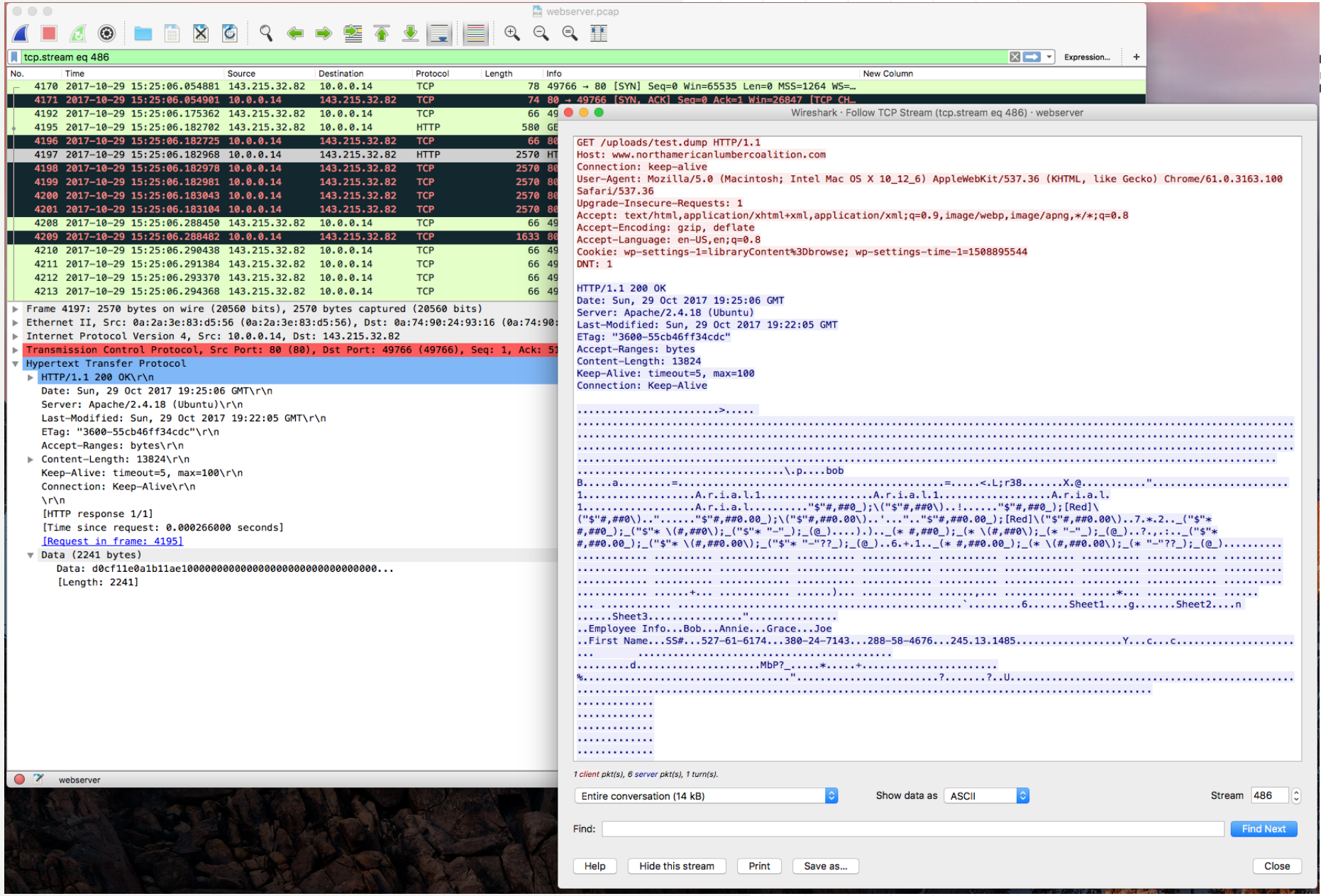
```
tulkas:309% file test                                                    ~/Desktop ]
test: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.2, Code page
: 1252, Author: bob, Last Saved By: bob, Name of Creating Application: Microsoft Excel, Creat
e Time/Date: Fri Oct 27 14:05:41 2017, Last Saved Time/Date: Fri Oct 27 14:07:17 2017, Securi
ty: 0
```



	A	B	C	D
1	Employee Info			
2	First Name	SS#		
3	Bob	527-61-6174		
4	Annie	380-24-7143		
5	Grace	288-58-4676		
6	Joe	245.13.1485		
7				
8				
9				
10				
11				
12				
13				
14				
15				

Rather interesting transfer. Was it exfiltrated?


tcp contains Grace
No. Time Source Destination Protocol Length
4197 2017-10-29 15:25:06.182968 10.0.0.14 143.215.32.82 HTTP
Frame 4197: 2570 bytes on wire (20560 bits), 2570 bytes captured (20560 bits)
Ethernet II, Src: 0a:2a:3e:83:d5:56 (0a:2a:3e:83:d5:56), Dst: 0a:74:90:24:93:16 (0a:7
Internet Protocol Version 4, Src: 10.0.0.14, Dst: 143.215.32.82
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49766 (49766), Seq: 1, Ac
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 29 Oct 2017 19:25:06 GMT\r\n
Server: Apache/2.4.18 (Ubuntu)\r\n
Last-Modified: Sun, 29 Oct 2017 19:22:05 GMT\r\n
ETag: "3600-55cb46ff34cdc"\r\n



Georgia Tech

CREATING THE NEXT®

Exfil

- 17:30-19:10 -- browsed around on connected drives and found a spreadsheet of Social Security Numbers
- 19:14 -- installed an upload.php script on the web server attempting to get the Social Security numbers onto webserver
- 19:22 -- installed netcat and transferred SSN spreadsheet to webserver using netcat
- 19:24 -- fetched test.dump (SSN spreadsheet) from external address
- 19:26 – encrypted web root to cover tracks