Chad Ballay

CYBR 420-342

10/18/2020

**Week 6**

For this section I’ll be using the Web Cache as my focus. Broadly speaking, Web Cache is agreed upon implementation of storing previously requested items. Usually images but any HTTP requestable object could be selected for storage. The major browser/OS have separate implementations for my example I’ll narrow the focus to Google Chrome on OS X. Browsing this data from the command line or file explorer does not yield anything that is obviously human readable. For this we can use third party applications most of which are closed source. Being able to see what sites the user has gone to and when they went to them provides a clear insight into what may have been a mis click or and act of intent.

* What the type of information is:

HTTP requestable items

* Where the information is stored with your browser (specify the browser you are using)

~/Library/Caches/Google/Chrome/Default/Cache/

* If and how the information can be erased by a user.

You can erase the information by loading chrome://settings/clearBrowserData in the URL bar of Chrome. From with in there you can select several items to clear besides the Web Cache.

* Why the information would be valuable in a forensics investigation.

**Email Headers**

For this part of the assignment we were to receive an email from the professor, review the email header, and then dissect the meaning of those headers.

Graphical user interface, text, application, email

Description automatically generated

For this I used the Office365 provided web client. It wasn’t immediately clear but with some effort I was able to use this submenu to see the email headers. “**View message details**”

Graphical user interface, text, application

Description automatically generated

This yielded this new layer on the webpage.

Graphical user interface, text, application

Description automatically generated

I’ve included the complete copy of the headers on a subsequent page. It is quite lengthy and there is much of it that isn’t relative to our needs.

For the analysis I first started off using the Google created tool for analyzing message headers.

<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

Graphical user interface, application

Description automatically generated

Which looks like Professor Geron used the Blackboard inbuilt tools to create and send the email to the class. I wouldn’t expect him using an AWS compute node as his personal email springboard. I also do not believe he would bounce his emails off of Blackboard unless it was involved in the process of the email.

But that is such a skin deep reading of the headers. For the first part you can see the individual stops along the way that the email took by looking at the “Headers”. Each stop along the message’s travel get an entry. Within that entry you have several key bits of information.

Time the event occurred.

Server name that the email was coming from.

Server name that the email was being sent to.

Received: from ip-10-145-94-141.ec2.internal (ec2-54-85-76-43.compute-1.amazonaws.com [54.85.76.43])

by mail-relay1-va2.blackboard.com (Sentrion-MTA-4.3.2/Sentrion-MTA-4.3.2) with ESMTP id 09DH4ngm017110;

Tue, 13 Oct 2020 17:04:49 GMT

Those three bits of information establish the hops the email travelled to get to us. DKIM and ESMTP have some overlapping duty on ensuring that the content of the email does not become modified in transit. (I’ll need more understanding before I can define that.) Finally, the message itself on the sending server is given an ID number that can be used for reference when researching the specific message across multiple server logs.

Message-ID: [989279158.25662.1602608695113.JavaMail.bbuser@ip-10-145-94-141](mailto:989279158.25662.1602608695113.JavaMail.bbuser@ip-10-145-94-141)

**EMAIL HEADERS**

Received: from CY1PR0801MB2266.namprd08.prod.outlook.com

(2a01:111:e400:c61b::12) by BY5PR08MB6406.namprd08.prod.outlook.com with

HTTPS; Tue, 13 Oct 2020 17:05:02 +0000

Received: from BN0PR02CA0009.namprd02.prod.outlook.com (2603:10b6:408:e4::14)

by CY1PR0801MB2266.namprd08.prod.outlook.com (2a01:111:e400:c61b::12) with

Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3455.21; Tue, 13 Oct

2020 17:04:57 +0000

Received: from BN8NAM12FT015.eop-nam12.prod.protection.outlook.com

(2603:10b6:408:e4:cafe::3a) by BN0PR02CA0009.outlook.office365.com

(2603:10b6:408:e4::14) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3455.29 via Frontend

Transport; Tue, 13 Oct 2020 17:04:57 +0000

Authentication-Results: spf=pass (sender IP is 69.196.241.1)

smtp.mailfrom=blackboard.com; my365.bellevue.edu; dkim=pass (signature was

verified) header.d=blackboard.com;my365.bellevue.edu; dmarc=pass action=none

header.from=blackboard.com;compauth=pass reason=100

Received-SPF: Pass (protection.outlook.com: domain of blackboard.com

designates 69.196.241.1 as permitted sender) receiver=protection.outlook.com;

client-ip=69.196.241.1; helo=mail-relay1-va2.blackboard.com;

Received: from mail-relay1-va2.blackboard.com (69.196.241.1) by

BN8NAM12FT015.mail.protection.outlook.com (10.13.183.188) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id

15.20.3477.11 via Frontend Transport; Tue, 13 Oct 2020 17:04:56 +0000

Received: from ip-10-145-94-141.ec2.internal (ec2-54-85-76-43.compute-1.amazonaws.com [54.85.76.43])

by mail-relay1-va2.blackboard.com (Sentrion-MTA-4.3.2/Sentrion-MTA-4.3.2) with ESMTP id 09DH4ngm017110;

Tue, 13 Oct 2020 17:04:49 GMT

DKIM-Filter: OpenDKIM Filter v2.7.5 mail-relay1-va2.blackboard.com 09DH4ngm017110

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=blackboard.com;

s=sep2018; t=1602608690;

bh=GT3yDCJx2sDFCEUF18FM/mybSEwBOFBZHATCw0IqPeU=;

h=Date:From:Reply-To:To:Subject;

b=KMTanmDky9ALQpZu3mOS6iwjyNY0+YbiEytHGk1ovqc7PSTk7rQWc+aBymveNHULc

r8u+1rC9lmheMXBRCO/78TRz/JGJiwenWL64wTRwJEFrEePLg+Y7plWOdjBp6OfwJK

YPsihGjWfR2dPrmHfMP5ITUKLDEAvjbo/mdb/OqJfHUQK4qIxjsjVhtQuPnhqBlv6L

7zjTLJ4SfuTq3wUR7VM5qt7lre7nO/w67hUbaFdfdjWgpMdkRBwhL9YCe84B57cyG1

pPXVjxFgfYT1qEAp0LUPJdp9cJyWY0hrEXXI3NiZaL7FljaskpPPgzKQG6i9m/CBPb

//A8jqRzRkyBQ==

Date: Tue, 13 Oct 2020 12:04:54 -0500 (CDT)

From: "Professor Anthony Geron - anthony.geron@bellevue.edu" <do-not-reply@blackboard.com>

Reply-To: "Professor Anthony Geron - anthony.geron@bellevue.edu" <anthony.geron@bellevue.edu>

To: "CYBR420-342N\_2211\_DD":;

Message-ID: <989279158.25662.1602608695113.JavaMail.bbuser@ip-10-145-94-141>

Subject: CYBR420-342N Cyber Investigations &amp; Forensi (2211-DD): Email

for Assignment

MIME-Version: 1.0

Content-Type: multipart/alternative;

boundary="----=\_Part\_25660\_507738363.1602608694212"

Return-Path: do-not-reply@blackboard.com

X-MS-Exchange-Organization-ExpirationStartTime: 13 Oct 2020 17:04:56.7545

(UTC)

X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit

X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000

X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit

X-MS-Exchange-Organization-Network-Message-Id:

7433671d-2764-4484-8f68-08d86f9a1c8c

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 26feded2-a083-4777-8052-06ad5ef53556:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-MS-PublicTrafficType: Email

X-MS-Exchange-Organization-AuthSource:

BN8NAM12FT015.eop-nam12.prod.protection.outlook.com

X-MS-Exchange-Organization-AuthAs: Anonymous

X-MS-Office365-Filtering-Correlation-Id: 7433671d-2764-4484-8f68-08d86f9a1c8c

X-MS-TrafficTypeDiagnostic: CY1PR0801MB2266:

X-LD-Processed: 26feded2-a083-4777-8052-06ad5ef53556,ExtFwd

X-MS-Exchange-Transport-Forked: True

X-MS-Exchange-Organization-SCL: -1

X-MS-Oob-TLC-OOBClassifiers: OLM:2150;

X-Microsoft-Antispam: BCL:1;

X-Forefront-Antispam-Report:

CIP:69.196.241.1;CTRY:US;LANG:en;SCL:-1;SRV:;IPV:NLI;SFV:SKN;H:mail-relay1-va2.blackboard.com;PTR:mail-relay1-va2.blackboard.com;CAT:NONE;SFS:;DIR:INB;

X-MS-Exchange-ABP-GUID: 487ba1c7-738f-4012-b52c-d45d9a5b4be6

X-MS-Exchange-ForwardingLoop:

ForwardingHandled;26feded2-a083-4777-8052-06ad5ef53556

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 13 Oct 2020 17:04:56.6856

(UTC)

X-MS-Exchange-CrossTenant-Network-Message-Id: 7433671d-2764-4484-8f68-08d86f9a1c8c

X-MS-Exchange-CrossTenant-Id: 26feded2-a083-4777-8052-06ad5ef53556

X-MS-Exchange-CrossTenant-AuthSource: BN8NAM12FT015.eop-nam12.prod.protection.outlook.com

X-MS-Exchange-CrossTenant-AuthAs: Anonymous

X-MS-Exchange-CrossTenant-FromEntityHeader: Internet

X-MS-Exchange-Transport-CrossTenantHeadersStamped: CY1PR0801MB2266

X-MS-Exchange-Transport-EndToEndLatency: 00:00:05.8247386

X-MS-Exchange-Processed-By-BccFoldering: 15.20.3477.020

X-Microsoft-Antispam-Mailbox-Delivery:

ucf:0;jmr:0;auth:0;dest:I;ENG:(750128)(520011016)(944506458)(944626604);

X-Microsoft-Antispam-Message-Info:

=?us-ascii?Q?iyAkU2vXap620LgE/jGSkHysOWI8+dUBu/b484Drq1I2FDl4yazhUKOBLGYh?=

=?us-ascii?Q?wtGViN4R6BVB6DV+pKX5D6JAYX1liUt0kqsc8UKwAIftAzQ9d7UiSmonfJ/k?=

=?us-ascii?Q?AdodT5h2shc6ELCac8MMEglhenbrERcPKbQes4dghW+tAdasfMVUSctG0sEv?=

=?us-ascii?Q?utT/WytFtaCvcAS6Fbi3m2/M9Co/RMhgjvV8MWnz/aLkUQyxUI9LA1GcuBFF?=

=?us-ascii?Q?bf7qiaLlZESCDSalQ2UyYboV+gD8mFHz40dtM9h5aquWsbNgy71jqGjbCJE6?=

=?us-ascii?Q?MlUnuxYmXQi2eSLmH70jUaOcLcimmM4cIdpXtVMoWmLcAM1aHzy2EOH8cgn+?=

=?us-ascii?Q?mmeC7Kvg/NUhb3jra28HVQP5C6VJCAr2InTROBMuOAibNBN+vzAs1ROfMEUL?=

=?us-ascii?Q?XL7GCC4o/kk04p0umzI6/P0IfCKM6fCky8CzFO2Vw0nppbjVipojb/l5p7XQ?=

=?us-ascii?Q?4pVCInsOEAX8UsyXjsCp7XUgifJfSLNrBRK8IAL/BWKx9DH2EIUDfDjPX5kD?=

=?us-ascii?Q?7QDvUrvA9c8P1pwzU2qxAze7e1/y5PIG7jjZUJ8QkaxnQxsgm13BZ14uPjtt?=

=?us-ascii?Q?Jw0OA2rShJlnP0xvezOkVhYJIrifEdr5cG3EAKCDYG5HZyD82RnTOGg+9POL?=

=?us-ascii?Q?TsagKd7kNhgV1X2+zwwgZTw5bzLoruAWvqQku+1HUrReNBjSkuA92QDLWquI?=

=?us-ascii?Q?0/LPndGCBd/9K7pXjtg/PrpLh00BdzvNBKa0ZLni/FCv4IwiYeKruvUuD32u?=

=?us-ascii?Q?rl1sp+gHlbUUYK/hUS6j8Bw9WELM/0G2SXunIlgfq9+95O1pYobRuPsvELyZ?=

=?us-ascii?Q?1rlrARSSiQuFyHlNRviVnL1JR0/nBotjJ0tzuiWWrs6Nkh4g0IlBPVQMRtTP?=

=?us-ascii?Q?svOvAKXD1ckFgE6UoFVr+wf0nve4+LNjT+H3/MbeppqGeHR8HpvJ7l72HI94?=

=?us-ascii?Q?4CcjgCpGKJrlBtnrImD3quGm1Msf67X43dzfsSGd9CtkQKztkASdPOF+bnzW?=

=?us-ascii?Q?E0W68T28DUhUIei8dHUfGfNicragb1abYKQKthj4pWCHE0smop9AxRReeIZy?=

=?us-ascii?Q?tPKzk5XPAQLUH3Rul+di+i/NbWGjkXd+VCh8qgliKrFAwarI6PzMF6zJwwuM?=

=?us-ascii?Q?6SB4STbmLAhJ995d+lub02eJtzXKLA7U2RVfB4L/SLQeYMW2LjImYYLvb8c1?=

=?us-ascii?Q?MqFCcDtegeZQ3pTWBuSnDxzdn6mWea0iX0ssJZH9dsQLlT2bi+3El6Do0Ks5?=

=?us-ascii?Q?DdV7ore7xlSDqWcLAp6Noa3pk5ZzfMb1LEC66SO4K1a9J9g4KRk5g3NrAndK?=

=?us-ascii?Q?Un945TtHoni8kg2aXa18R+padEobiTk/hBqurJ/iWMwE8yb21uLWTKjr/7uI?=

=?us-ascii?Q?+Ox2bApa1ySHooLIwaF6aobjsYwj5FUqOVpljjkTB1V+TfEUew=3D=3D?=