Forensic Investigation of Emails Altered on the Server
Background

Arman Gungor
Founder, Metaspike
@ArmanGungor
www.metaspike.com
Altering Emails on The Server

Upcoming Purchase

FD
To info@prokimit.com

Hello,

Please proceed with the transaction immediately. Thank you.
Altering Emails on The Server

Upcoming Purchase

FD  FEC Dev <fecevdev@yahoo.com>
To info@precosini.com

Hello,

Please proceed with the transaction immediately. Thank you.
Sync to Server

- **APPEND**: Add new message to mailbox
- **UID STORE**: Set deleted flag
- **UID EXPUNGE**: Remove old message from mailbox
Recovering the Original Message
Exchange / O365

- Recoverable Items Root
  - Audits (635)
  - Calendar Logging (30)
  - Deletions (419)
  - DiscoveryHolds (0)
  - Purges (219)
  - Versions (0)
Altering Emails on The Server
Suspect Message on GoDaddy

Upcoming Purchase

FEC Dev [fecdev@yahoo.com]
Sent: 1/15/18 11:58 am
To: info@proksimiti.com

Hello,

Please cancel the transaction immediately. Thank you.
Suspect Message on GoDaddy

Upcoming Purchase

FEC Dev [fecd@yahoocom]

Sent: 1/15/18 11:58 am
To: info@proksimiti.com

Hello,

Please cancel the transaction immediately. Thank you.
Suspect Message on GoDaddy

Upcoming Purchase

FEC Dev [fecdev@yahoo.com]
Sent: 1/15/18 11:58 am
To: info@proksimiti.com

Hello,

Please cancel the transaction immediately. Thank you.
How to Preserve

- Internet Message Format (RFC 5322)
- Server metadata
- Context
Server Metadata

- Information about the messages
- Kept on the server
- Typically not acquired with the messages
Access to Email Evidence

- Access to printout of email
- Access to email in native/near-native format
- Access to email account on the server
- Access to entire email server
Access to Email Evidence

- Access to printout of email
- Access to email in native/near-native format
- Access to email account on the server
- Access to entire email server

Server metadata
IMAP Server Metadata

- Unique Identifier (UID) Message Attribute
- Flags Message Attribute
- Internal Date Message Attribute
Unique Identifier (UID) Message Attribute

- Unique 32-bit value that identifies a message within a mail folder
- Assigned in an ascending fashion
- Not necessarily contiguous
Internal Date Message Attribute

- Internal date/time of the message on the server
- Reflects creation within the mail folder
  - SMTP — Time of final delivery
  - IMAP COPY — Timestamp of source message (COPY should preserve internal date and flags; sets \Recent flag on the copy)
  - IMAP APPEND — Timestamp argument or time of APPEND
Server Metadata before Manipulation

Received: (qmail 27394 invoked by uid 30297); 15 Jul 2019 19:00:53 -0000
...<SNIP>...
Date: Mon, 15 Jul 2019 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="--_Part_915725_248640444.1563217119409"
References: <660010183.915726.1563217119410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.13991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700

Hello,
Please proceed with the transaction immediately. Thank you.

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:16px;">

Hello,

Please proceed with the transaction immediately. Thank you.

</div></body></html>
Hello,
Please cancel the transaction immediately. Thank you.

--=_Part_915725_248640444.1563217119409
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

<hl>Hi</hl>

<br>

Please cancel the transaction immediately. Thank you.

--=_Part_915725_248640444.1563217119409

Hello,
Please cancel the transaction immediately. Thank you.

--=_Part_915725_248640444.1563217119409

---=_Part_915725_248640444.1563217119409
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div class="yahoo-style-wrap" style="font-family:Helvetica Neue, Helvetica, Arial, sans-serif;font-size:16px;" data-set-dir="false">Hello,""
</div><div dir="ltr" data-set-dir="false">Please cancel the transaction immediately. Thank you</div><div dir="ltr" data-set-dir="false">."
</div></div></body></html>
Hello,
Please cancel the transaction immediately. Thank you.
Gmail Server Metadata

- threadId
- labelIds
- historyId
  - labelAdded
  - labelRemoved
  - messageAdded
  - messageDeleted
- internalDate — can reflect Date header for API-migrated mail
Message Data & Metadata

- Acquired with the message
  - Message-ID
  - In-Reply-To
  - References
  - Trace Fields
  - Content-Length
  - X-Originating-IP
  - DKIM Signatures
  - MIME boundary delimiters
  - and more...

Date: Tue, 05 Mar 2019 16:18:36 +0000
Message-ID: <E1.58.01884.C51AE7C5@momentum-coi- mta3.prod.aweberint.com>
From: “Arman Gungor” <agungor@example.com>
Subject: Forensic Exam
To: jdoe@example.com
Received: (qmail 27394 invoked by uid 30297); 15 Jan 2018 19:00:53 -0000
Received: from unknown (HELO p3plbsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
   (envelope-sender <fecdev@yahoo.com>)
   by p3plbsmtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
   for <info@proksimiti.com>; 15 Jan 2018 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
   (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
   (Client did not present a certificate)
   by CMGW with ESMTP
   id n6DUhF6dMOy6n6DUhGMC; Mon, 15 Jan 2018 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com;
   s=s2048; t=1563217240; bh=8X7yayAlb3rM/ntRAK51gp9Em0JURK/p+ksVuZ55IU=;
   h=Date:From:To:Subject:References:From:Subject;
   b=tQ1O9lbhlhas/87XFpUnlyshU7yZdVm4L4CMc6HyicfFz+jsIT5u5yAQB9fwiiilaEY4Q6aTGK1Bjn3WI967WUwAN0d4uYide8NWmL1uSz54p68muVqV8SrkbwEDlxL7
deohpTglip373841skgWw4BiqKg9b552RaBa+0yHyRlCe44/T5zOApcy1Ps22LAdjyrXgfIrudxle93sJUJcUcvaT4Esp3SU7+nQK9aMb7IHyCGhaDJNCn7c+yclcxC
Neag54Qqmi1OQj02Kvq8i5rj/D2mgSj02ikGYOjiM28GtQZcsRgsQ9UsvIn9a5bS5TGvgvBA==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.bf2.yahoo.com with HTTP; Mon, 15 Jan 2018 19:00:40 +0000
Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
   boundary="-----=_Part_915725_248640444.1563217119409"
References: <660010183.915726.1563217119410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.133991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700
Content-Length

- Byte size of message payload
- Windows (CR/LF) v. Unix (LF)
Received: (qmail 27394 invoked by uid 30297); 15 Jan 2018 19:00:53 -0000
Received: from unknown (HELO p3plsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
  (envelope-sender <fecdev@yahoo.com>)
  by p3plsmtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
  for <info@proksimiti.com>; 15 Jan 2018 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
  (Client did not present a certificate)
  by CMGW with ESMTP
id n6DUhF6dMOyion6DUhGLMC; Mon, 15 Jan 2018 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240;
bh=8X7yayAIb3rM/ntRAK51gp9Em0JURK/p+kSVu/J55lU=;
  h=Date:From:To:Subject:References:From:Subject
  b=tQ1O9lbhlhas/87XFppUNly5sUHyzDvM4L4M6i6i6cfzj+iTs5u5yAQ89fNwmiiaEE4QOaTG1BhJn3Wi967WUwnAN0d4Yu8NwM1uSz4p68muVq4Y8PrbwEDILxL7
deohpTgpI93T8415skbGWW4BisqG9b52RaBa+b4yHrDICe4aTSz0ApC1Psw22LAjdjrYXgifnruNuxde193s/RUcUCvaT4Esp3bSU7+nQK9aMw7IHyCghaDJNCn7c+yLceCNea5QOqm1OQlo2Kvq88Sr9j/D2mgSj02iKYDj15M2B97GQ2cRsQsdvflvIN9a5f5T6g8vb8A==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.bf2.yahoo.com with HTTP; Mon, 15 Jan 2018 19:00:40 +0000
Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.156321719410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary=""-----=_Part_915725_248640444.156321719409"
References: <660010183.915726.156321719410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.13991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700
Should be 688
Received: (qmail 27394 invoked by uid 30297); 15 Jan 2018 19:00:53 -0000
Received: from unknown (HELO p3plsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
  (envelope-sender <fecdev@yahoo.com>)
  by p3plsmtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
  for <info@proksimiti.com>; 15 Jan 2018 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
  (Client did not present a certificate)
by CMGW with ESMTP
id n6DUhF6dMOiyon6DUhGLMC; Mon, 15 Jan 2018 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240; bh=8X7yayAIb3rM/ntRAK51gp9Em0JURK/p+ksVu/25SIU=;
h=Date:From:To:Subject:References:From:Subject;
b=tQ1O9iblhlhas/87XFPpUNllysUhlzDvM42L4MC6i6icfFZj+iJi5Tu5yaQ8B9fxxnii6EY4Q6aT6GK1Bjn3W5i967WUwAN0d4uye8NwM1u5Sz4p68muVq8SVpkrbwEDlxl7
depohTgI9Ilt845iskbGWw4Bisqk9G9b52RbaB+a+HyYdrCie4a/T5sz0AprC1Yps22LAIjd75X7Pyfmynudkxieh93s/4UjCUCaT4Esp3bSU7+nQK9aM6blHyCGhaDJNCn7c+y1lC
Nee954Qmb10Qjo2Kvq8isSrh/D2mgSJ02iGY0ij3M28GtQczRsQsduflvin9a5f557DgqvBA==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.bf2.yahoo.com with HTTP; Mon, 15 Jan 2018 19:00:40 +0000
Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="----=_Part_915725_248640444.1563217119409"
References: <660010183.915726.1563217119409.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.13991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700

Should be 688

Fails DKIM

EPOCH Date: Mon, July 15, 2019 18:58:39.409 (UTC)
Altered Message Header

Received: (qmail 27394 invoked by uid 30297); 15 Jan 2018 19:00:53 -0000
Received: from unknown (HELO p3plsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
  (envelope-sender <fecdev@yahoo.com>)
  by p3plsmtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
  for <info@proksimiti.com>; 15 Jan 2018 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
  (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
  (Client did not present a certificate)
  by CMGW with ESMTP
  id n6DUhF6dMOyjon6DUhGLMC; Mon, 15 Jan 2018 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240; bh=8X7yayAlb3rM/ntRAK51gp9EmOJURK/p+ksVu/2SIU=;
h=Date:From:To:Subject:References:From:Subject;
b=tQ1O9ltbhlas/87XFppUNllysUhYZvM42LM6C6i6icf2+zjSTSu5yAQB9fwxiiaEY4Q6aTgK1Bjn3WI967WUwAN0d4uYide8NW1MuSz4p68muVqV8SPrkbwEDlx17deohpTgiI93T84I5skBGiWw4Bisug9bS2RaBa+QyHydRiCe4aAT5zOAprCyPsw22LaIdjrXyGfnrudxie93s/uJcUCvaT4Esp3b5SU7+nQK9aMb7bHyCGhaDJNCN7c+yjcxCNea54QQmn10Qio2Kqvg8l5rj/D2mgSj02KGYOjIM28GtQ2csRgQsdufviN9a5f5TdGvg8A==
Fails DKIM

Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary=""--==--Part_915725_248464.44.1563217119409"
References: <660010183.915726.1563217119410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.133991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700

EPOCH Date: Mon, July 15, 2019 18:58:39.409 (UTC)
EPOCH Date: Mon, July 15, 2019 18:58:39.410 (UTC)
Should be 688
Altered Message Header

Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary=""_Part_915725_248640444.1563217119409"
References: <660010183.915726.1563217119409.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.133991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240; bh=8277yayAlb3rM/hTRAK51gp9Em0JURK/p+ksVu/2JSIU=; h=Date:From:To:Subject:References:From:Subject
b=tQ1O9lbhlhas/87XFpUUnylsyUjkDyVzmi42LMC6f1of22+jisTi5u5yAQ8f7wmiilwEO4QaTGk1Bjn3WJ967VUwAN0d4Yide8NwM1usz4p68muVq85PrkbwEDlxLT7
dehopTgl93T845skbGlw4Bisqg9bS2Ra8a+9yHydRle4e4/tTsz0Apc1Ypsw2LAljdYrXygfrnudxe93s/ruJcUCvaT4Esp3bSU7+nQk9aMb7IHyCGhaDJNCn7cy+yCx
Nea54QQmio1Oqlo2Kq8gB5rgh/D2mgSjO2kGYOJiM28GtQzcsRgQs0dufwiN9a5bStDgvg8A==

EPOCH Date: Mon, July 15, 2019 7:00:40 PM (UTC)
Fails DKIM

EPOCH Date: Mon, July 15, 2019 18:58:39.410 (UTC)

EPOCH Date: Mon, July 15, 2019 18:58:39.409 (UTC)

EPOCH Date: Mon, July 15, 2019 7:00:40 PM (UTC)
Altered Message Header

Received: (qmail 27394 invoked by uid 30297); 15 Jan 2018 19:00:53 -0000
Received: from unknown (HELO p3p1bsmtp02-01.prod.phx3.secureserver.net) ([68.178.213.1])
   (envelope-sender <fecdev@yahoo.com>) by p3p1smtp15-02-25.prod.phx3.secureserver.net (qmail-1.03) with SMTP
   for <info@proksimiti.com>; 15 Jan 2018 19:00:53 -0000
Received: from sonic306-30.consmr.mail.bf2.yahoo.com ([74.6.132.229])
   (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits)
   (Client did not present a certificate)
   by CMGW with ESMTP
   id n6DUhF6dMOyon6D0UHGLMC; Mon, 15 Jan 2018 12:00:53 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1563217240; bh=8X7yayAIb3rM/ttRAKs1gp9Em0JURK/p+ksVu/2SSJU=;
h=Date:From:To:Subject:References:From:Subject;
b=Q1Q9iblihas/87XFpPNvlYlsUhYzDvMi42LMc6I6icofZ2+jiST5u5yAQBF9xwniiaa4Y4Q6aTGK1Bj3W9i67WUwAN0d4uYide8NwM1uSzD4p68muVqv85PrkbwEDi-xl7
depofTgi93T84i5sk3GW4Bisqg9b52RbaA+qBYWdRcele4/1T5szOaEyc1Ypsw22LAldjyrXgfRnuDxie93s/JUcUCvaT4EsPl3bSU7+snQK9aMb7lHyCGhaDINcN7c+yIxrC
NeaS4QQm1iQlo2KvqgBirj8rj/D2mgSj02kIYyJiM8OgtQ2cRgsQ5duflvIN9a5bfSTGvgBAA==
Received: from sonic.gate.mail.ne1.yahoo.com by sonic306.consmr.mail.bf2.yahoo.com with HTTP;
   Mon, 15 Jan 2018 19:00:40 +0000
Date: Mon, 15 Jan 2018 18:58:39 +0000 (UTC)
From: FEC Dev <fecdev@yahoo.com>
To: "info@proksimiti.com" <info@proksimiti.com>
Message-ID: <660010183.915726.1563217119410@mail.yahoo.com>
Subject: Upcoming Purchase
MIME-Version: 1.0
Content-Type: multipart/alternative;
   boundary="---=Part_915725_248464_44.1563217119409"
References: <660010183.915726.1563217119410.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.133991 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Length: 700

Should be 688
Altered Message Body

Hello,
Please cancel the transaction immediately. Thank you.
DKIM Verification

- Perl—Mail::DKIM::Verifier
- Python—dkimpy
- Manual verification
Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E00002525000000006AFF0005EDE3B80

- 22-byte header
- 0 or more 5-byte child blocks
Conversation Index

Date (FILETIME)
02/04/2019 22:39:06.7151360 (UTC)

GUID
4d871898-8e9f-407d-b016-4af82711a59e
Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E 0000252500 000006AFF0 005EDE3B80

CHILD 1

Time Difference: 00:04:09.2727296

02/04/2019 22:43:15.9878656 (UTC)
Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E 0000252500 000006AFF0 005EDE3B80

CHILD 2

Time Difference: 00:00:44.8528384

02/04/2019 22:44:00.8407040 (UTC)
Conversation Index

01D4BCDA6FEB4D8718988E9F407DB0164AF82711A59E
0000252500
000006AFF0
005EDE3B80

Time Difference: 1.21:16:22.1337600
02/06/2019 20:00:22.9744640 (UTC)
Takeaways

- Preserve in the original format
- Capture server metadata
- Acquire & examine in context