Digital Forensics in Google

CHRIS THOMAS

DESKTOP ENGINEER - INGHAM ISD

CTHOMAS@INGHAMISD.ORG

@AUTOMATEMYSTUFF

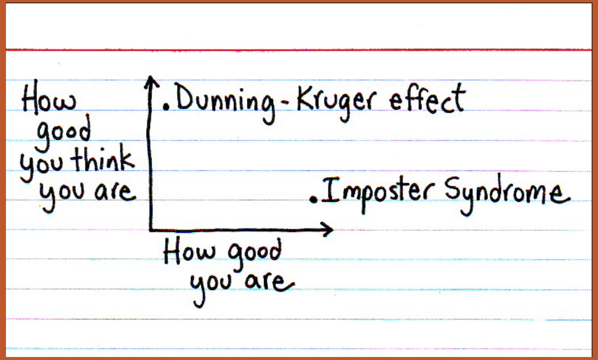
Ingham Intermediate
School District
A Regional Educational Service Agency

Session Description

My hope is that this session can give everyone a brief look at each administrative tool you have available in Google Workspace while presenting you with some examples of issues I’ve worked on in the past and then leave you feeling more confident that you can use data to form a narrative for your administrators.

The goal in the process is to collect objective data/evidence to support or oppose a narrative about the situation you are investigating.

Scenarios presented may or may not have been actual tickets.



Who Am I?

- 20 Years In K12 Technology
  - Intern, Tech, Coordinator, Engineer
- Lifelong Learner
  - /r/sysadmin, /r/k12sysadmin, RSS feeds
- Relentlessly Inquisitive
  - Let's Ask The WinAdmins Slack
- Problem Solver
  - Professional Googler
- Voracious Reader
  - docs.microsoft.com
- Community Minded
  - MAEDS, MISCUG, WMISMUG
- #ImpostorSyndromeBeDamned

Past Presentations

2013 MAEDS Fall Conference
Attended 'Marketing Yourself' by Kris Young and Kevin Galbraith
"Our Name, Reputation and Skill Sets Need to be KNOWN"

2014 MAEDS Spring PD Day
First time presenting and it's a 'ConfigMgr panel' for a half day session.

2014 MAEDS Fall Conference
Presented 'PADT and SCCM'

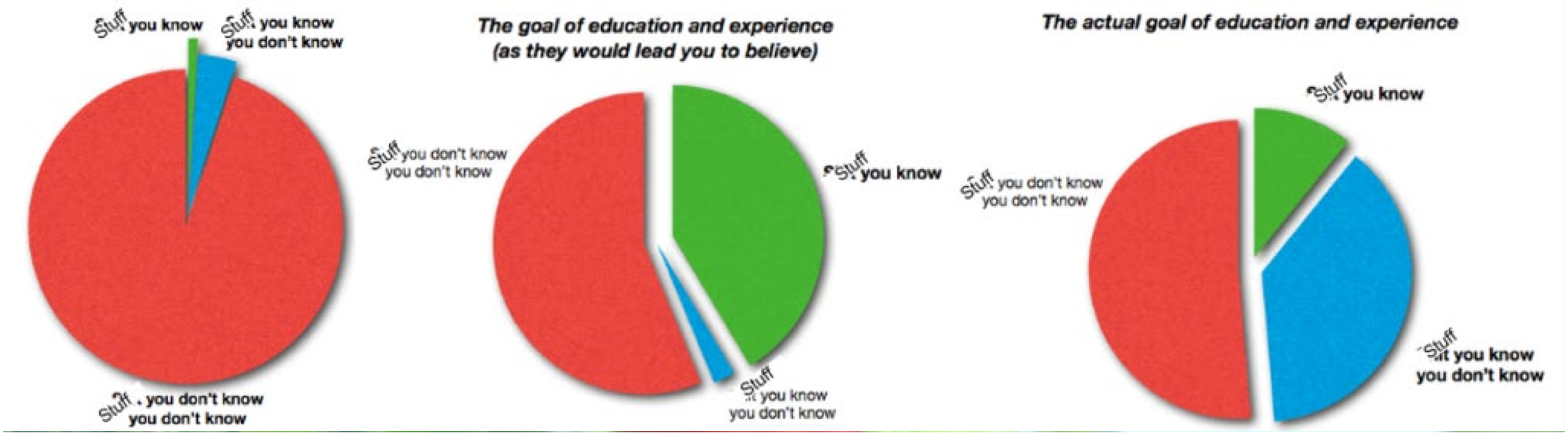
2015 MAEDS Spring PD Day
Presented 'ConfigMgr panel' for a half day session.

2015 MAEDS Fall Conference
Presented 'Automate ALL THE THINGS with PowerShell App Deployment Toolkit'

2017 MAEDS Fall Conference
Presented 'PowerShell – Intro session for those that have been too afraid to take the plunge'

2018 MAEDS Fall Conference
Presented 'PowerShell - Intermediate Session for Those That Overcame Their Fears and Took the Plunge'

2019 MACUL Conference
Presented 'Office 365 Administration'



No One Know What the F*** They're Doing (or "The 3 Types of Knowledge")

Steve Schwartz – May 13, 2010

https://www.bridge-global.com/blog/3-types-of-knowledge/

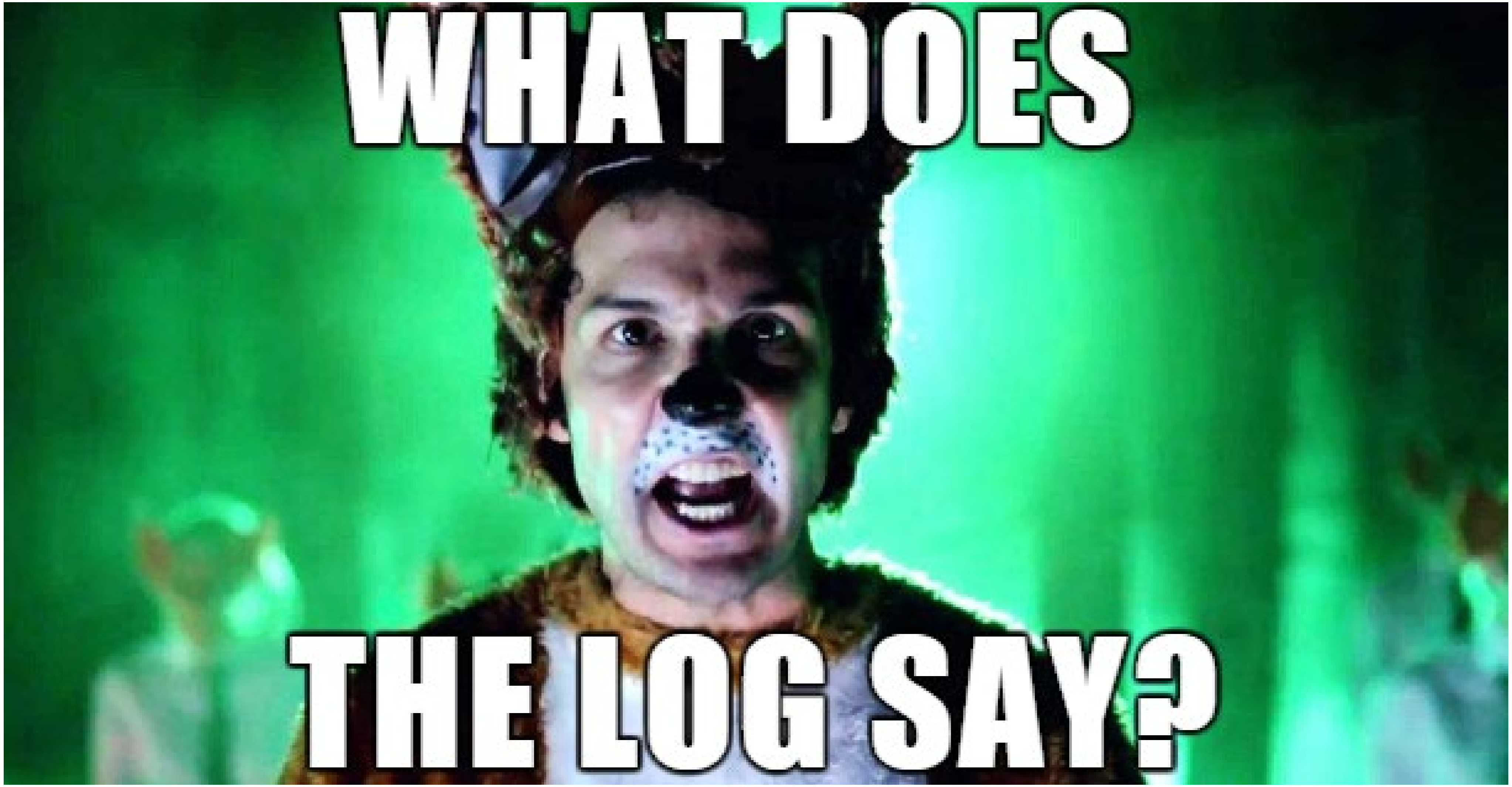
Be The Master

"Teaching does not always feel rewarding. It doesn't need to be. It is a repayment of something that was done for you. It is not a good thing that you do; it is an obligation that you have."

https://donjones.com/2017/10/19/become-the-master-or-go-away/

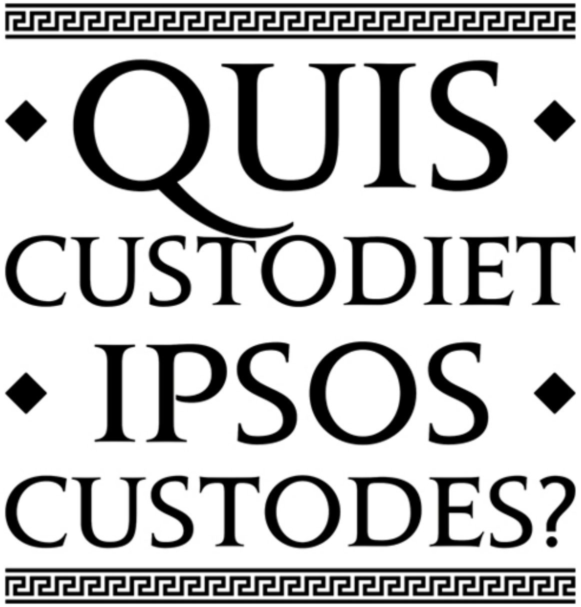
"Manning Books has signed me up to write ~~Master Your Technology Career~~ Own IT, which will include much of the narrative and content from these prior books. That content will be re-cast slightly to be more specific and actionable to a technologist audience. The new book will also bring in a metric butt-tonne of new content around key soft skills, professionalism, personal branding, job hunt foundations, and a lot more."

https://donjones.com/2020/07/27/more-details-the-fate-of-be-the-master-and-lets-talk-business/


WHAT DOES
THE LOG SAY?

Audit Log

- Unlike Microsoft, which requires admins to enable audit log search before it’ll start collecting administrative actions to audit … Google has it on by default.
- Available Audit Logs
  - Admin Audit Log
  - Login Audit Log
  - User Accounts Audit Log
  - Drive Audit Log
  - Google Meet Audit Log
    - Use Google Meet Quality Tool instead.
  - Groups Enterprise Audit Log
    - Wait… When did I get this?!
- Email Log Search



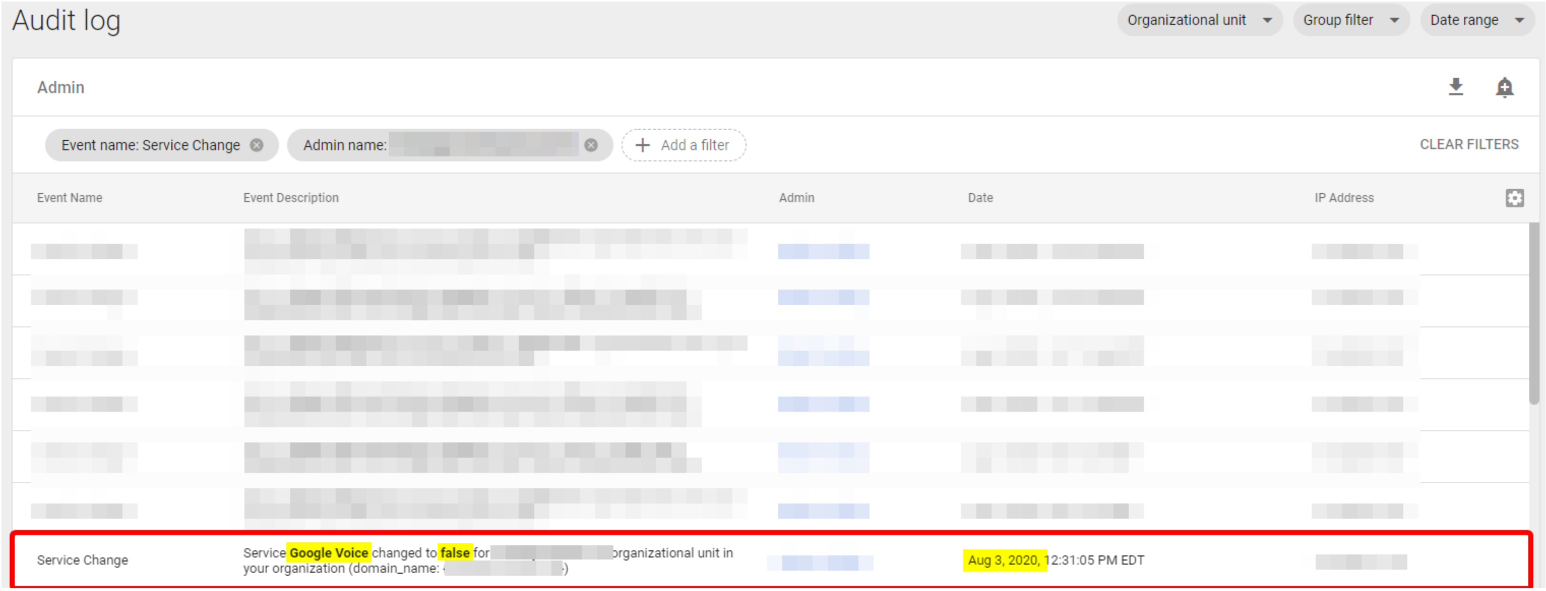
Admin Audit Log Scenario

User creates ticket in January 2021 indicating that they've been using their school account to stay in contact with families through text and voice while obfuscating their personal cell phone number with Google Voice, but it stopped working yesterday.

You run an Admin Audit Log search for 'Service Change' events and find the Google Voice service was disabled for the whole domain by an admin in August of 2020.

August. Of. 2020.

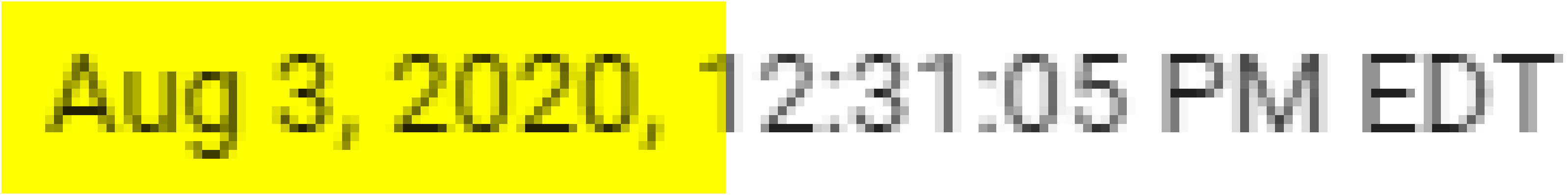
Not Yesterday.



Event name: Service Change

Admin name: [redacted]

Event Name	Event Description	Admin	Date	IP Address
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Service Change	Service Google Voice changed to false for [redacted] organizational unit in your organization (domain_name: [redacted])	[redacted]	Aug 3, 2020, 12:31:05 PM EDT	[redacted]



Aug 3, 2020, 12:31:05 PM EDT

Google Vault / eDiscovery

What is Google Vault?

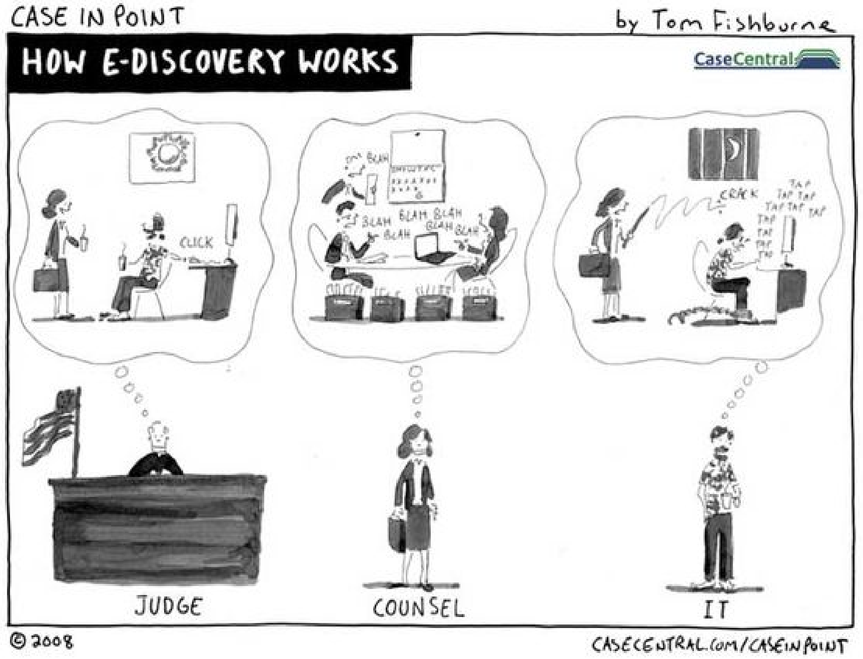
- https://support.google.com/a/answer/2462365?hl=en

“Vault is an information governance and eDiscovery tool for Google Workspace. With Vault, you can retain, hold, search, and export users’ Google Workspace data. You can use Vault for the following data:

- *Gmail messages*
- *Drive files*
- *Google Chat messages (history turned on)*
- *Google Meet recordings and associated chat, Q&A, and polls logs*
- *Google Groups messages*
- *Google Voice for G Suite text messages, voicemails and their transcripts, and call logs*
- *Classic Hangouts messages (history turned on)”*

https://vault.google.com/

http://ediscovery.google.com/ (classic Vault)


CASE IN POINT
by Tom Fishburne
HOW E-DISCOVERY WORKS
CaseCentral
CLICK
BLAH BLAH BLAH BLAH BLAH BLAH
CRACK
TAP TAP TAP TAP TAP TAP TAP TAP TAP TAP
JUDGE
COUNSEL
IT
© 2008
CASECENTRAL.COM/CASEINPOINT

Acronyms/Slang

AITR: Adults In The Room

POS: Parents Over Shoulder

KYS: Kill Yourself

KMS: Kill Myself

KMN: Kill Me Now

THOT: That Ho Over There

TDTM: Talk Dirty To Me

WUD/WYD: What You Doing?

53x: Sex

Bae: significant other, “before anyone else”

Bet: “yes” or “watch me”

Ghost: purposely ignore someone

Troll(ing): intentional harassment, criticizing or antagonizing of someone

Swat(ing): making a false report to elicit response from law enforcement

Catfishing: fake identity to target a victim online

Imping: Impersonating someone online in order to embarrass them

Salty: Someone upset by something

Emojis/Kaomoji

Chromebook

https://support.google.com/chromebook/answer/6076237?hl=en#zippy=%2Cinsert-emoji-or-other-images

Windows 10

https://support.microsoft.com/en-us/windows/windows-10-keyboard-tips-and-tricks-588e0b72-0fff-6d3f-aeee-6e5116097942

iOS

https://support.apple.com/en-us/HT202332

Android

https://support.google.com/gboard/answer/2842292?co=GENIE.Platform%3DAndroid&hl=en

Threatening

- 👊👉🚑🔪🔫💀

Racism

- 🍉🍗🐵👌

Sexual

- 👄✊💦🍆🍑😈🌮

Risky/Illegal

- 🍁🥦💊💉⛷

Kaomoji

- (╯°□°) ╯︵ ┻━━┻
- (-_･) ︻デ═一 ▸

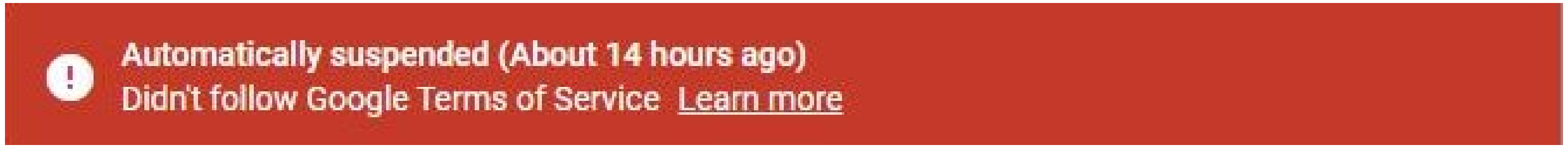
eDiscovery / Google Vault Caveat Scenario

User creates ticket indicating that a student account cannot login to their Chromebook or any Google services, like Google Classroom or Google Meet.

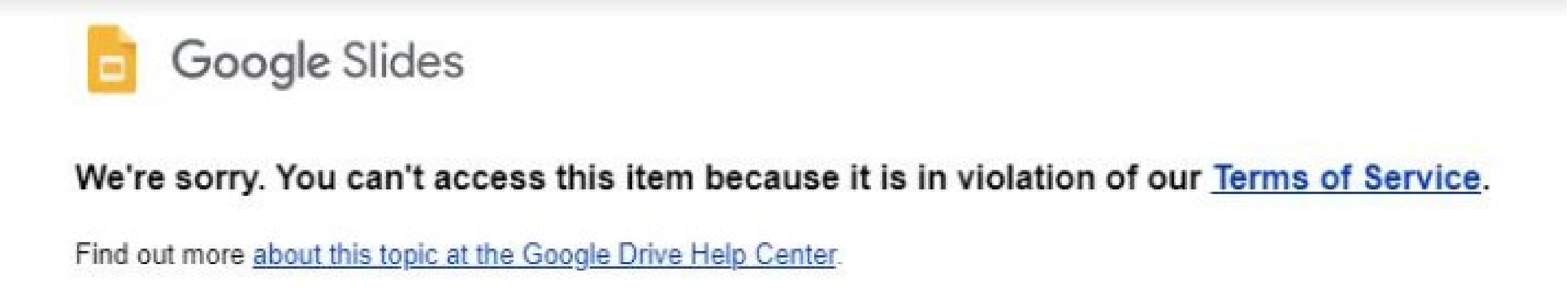
Help Desk validates student account is suspended, but they are unable to unsuspend the account.

You engage Google Support to find that **they** cannot unsuspend the account and must escalate. Yet, escalations will give you no explanation.

Whatever, let’s make a new student account and recover their data from eDiscovery / Google Vault.



Automatically suspended (About 14 hours ago)
Didn't follow Google Terms of Service Learn more



Google Slides

We're sorry. You can't access this item because it is in violation of our Terms of Service.

Find out more about this topic at the Google Drive Help Center.

Anyone out there backing up your Google Drive data? Risk/Reward Benefit?

YouTube

- No Vault / eDiscovery
  - No retention of data
- Lack of administrative tools other than approved videos feature.
- Limited support as an “Additional Google services”
- Curriculum ONLY stored in YouTube?
  - What do you do if a user violates TOS and gets account suspended as I mentioned earlier?
  - What do you do if a user accidentally deletes videos?
  - What do you do if a disgruntled user deletes videos and/or channel on purpose?

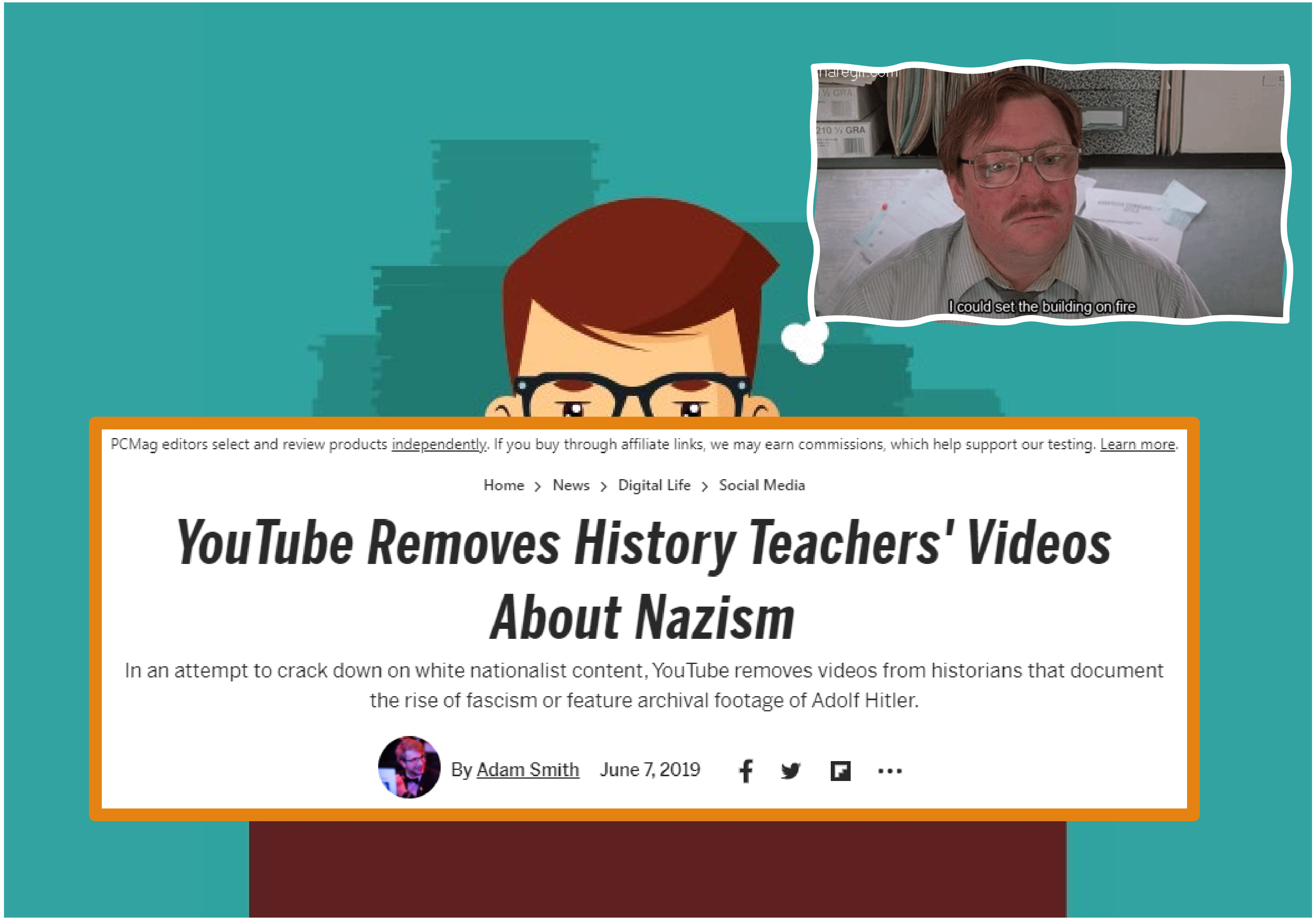
YouTube Scenario

User creates ticket indicating a YouTube channel is no longer working and they need those videos for their curriculum that is shared with multiple teachers.

You find that the teacher who created these videos was disgruntled and had deleted their channel while handing in their letter of resignation.

Through engagement with Google Support you learn that there is **zero** they can do to help you and this product isn't supported in Vault.

Or… the user abuses TOS and Google removes the video/channel.



PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing. Learn more.

Home > News > Digital Life > Social Media

YouTube Removes History Teachers' Videos About Nazism

In an attempt to crack down on white nationalist content, YouTube removes videos from historians that document the rise of fascism or feature archival footage of Adolf Hitler.

By Adam Smith June 7, 2019

Google Drive / Docs / Slides / Sheets

- Shared Docs to chat in
- Siblings in unique living arrangements discuss things
- Comments as communication
- Chat within applications

Google Drive / Docs / Slides / Sheets Scenario

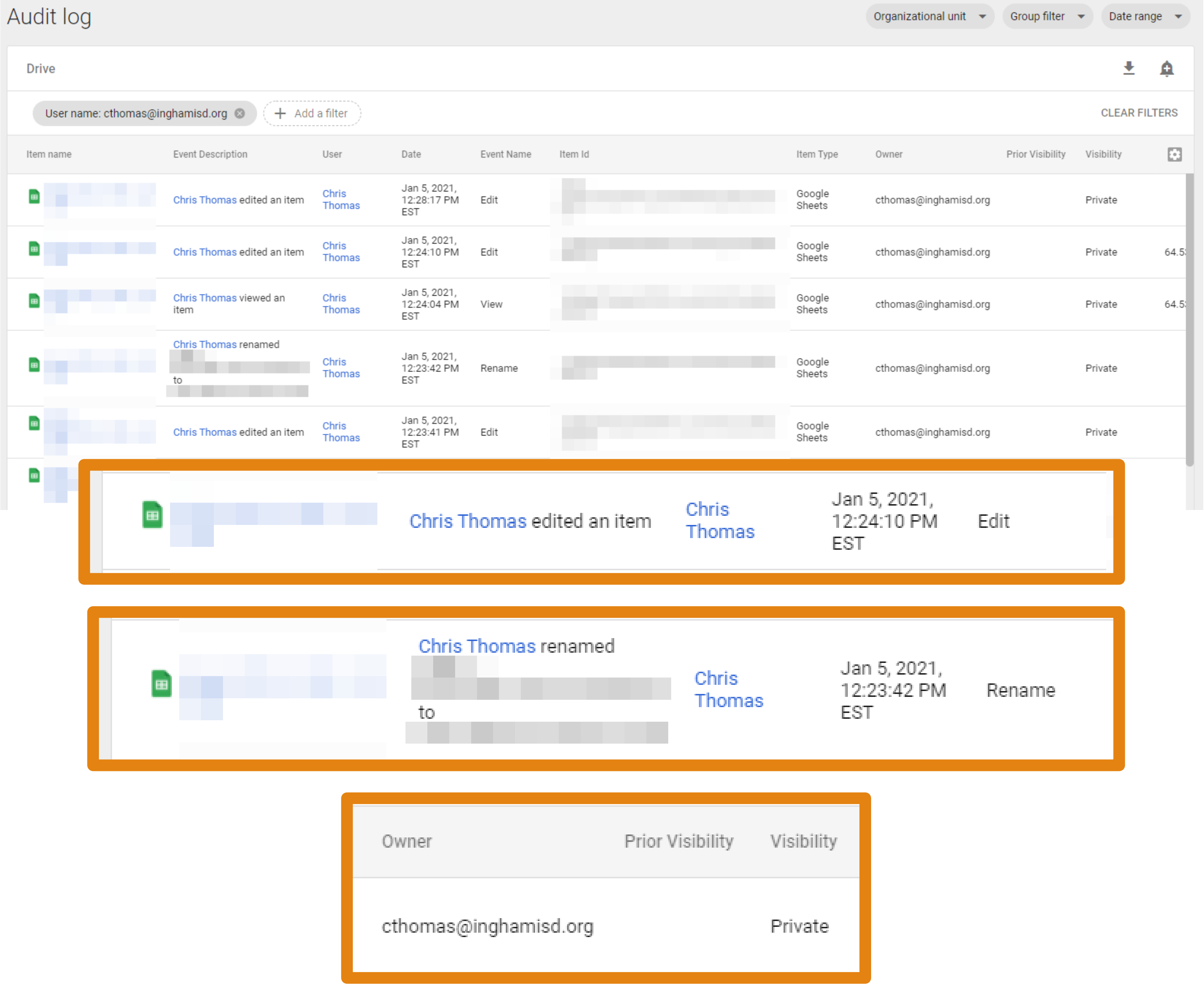
User creates ticket indicating student has run away from home and asks if there is anything you can do to help locate the student.

You find no Login Audit Log activity for the student account that would be helpful. However, maybe you run Drive Audit Log search looking for …

… recent file edits…

… or recent file renames …

… and you can look into the owner/visibility of that file.



User name: cthomas@inghamisd.org

Item name	Event Description	User	Date	Event Name	Item Id	Item Type	Owner	Prior Visibility	Visibility	
[redacted]	Chris Thomas edited an item	Chris Thomas	Jan 5, 2021, 12:28:17 PM EST	Edit	[redacted]	Google Sheets	cthomas@inghamisd.org		Private	
[redacted]	Chris Thomas edited an item	Chris Thomas	Jan 5, 2021, 12:24:10 PM EST	Edit	[redacted]	Google Sheets	cthomas@inghamisd.org		Private	64.5
[redacted]	Chris Thomas viewed an item	Chris Thomas	Jan 5, 2021, 12:24:04 PM EST	View	[redacted]	Google Sheets	cthomas@inghamisd.org		Private	64.5
[redacted]	Chris Thomas renamed [redacted] to [redacted]	Chris Thomas	Jan 5, 2021, 12:23:42 PM EST	Rename	[redacted]	Google Sheets	cthomas@inghamisd.org		Private	
[redacted]	Chris Thomas edited an item	Chris Thomas	Jan 5, 2021, 12:23:41 PM EST	Edit	[redacted]	Google Sheets	cthomas@inghamisd.org		Private	
[redacted]										

Item name	Event Description	User	Date	Event Name
[redacted]	Chris Thomas edited an item	Chris Thomas	Jan 5, 2021, 12:24:10 PM EST	Edit

Item name	Event Description	User	Date	Event Name
[redacted]	Chris Thomas renamed [redacted] to [redacted]	Chris Thomas	Jan 5, 2021, 12:23:42 PM EST	Rename

Owner	Prior Visibility	Visibility
cthomas@inghamisd.org		Private

GMail / Chat

- eDiscovery
- Chat history is stored in GMail
- Partially completed thoughts from auto-saves, erase and redo thoughts
- Reports -> email log search (https://admin.google.com/AdminHome?hl=en#Reports:subtab=email-log-search)

GMail / Chat Scenario

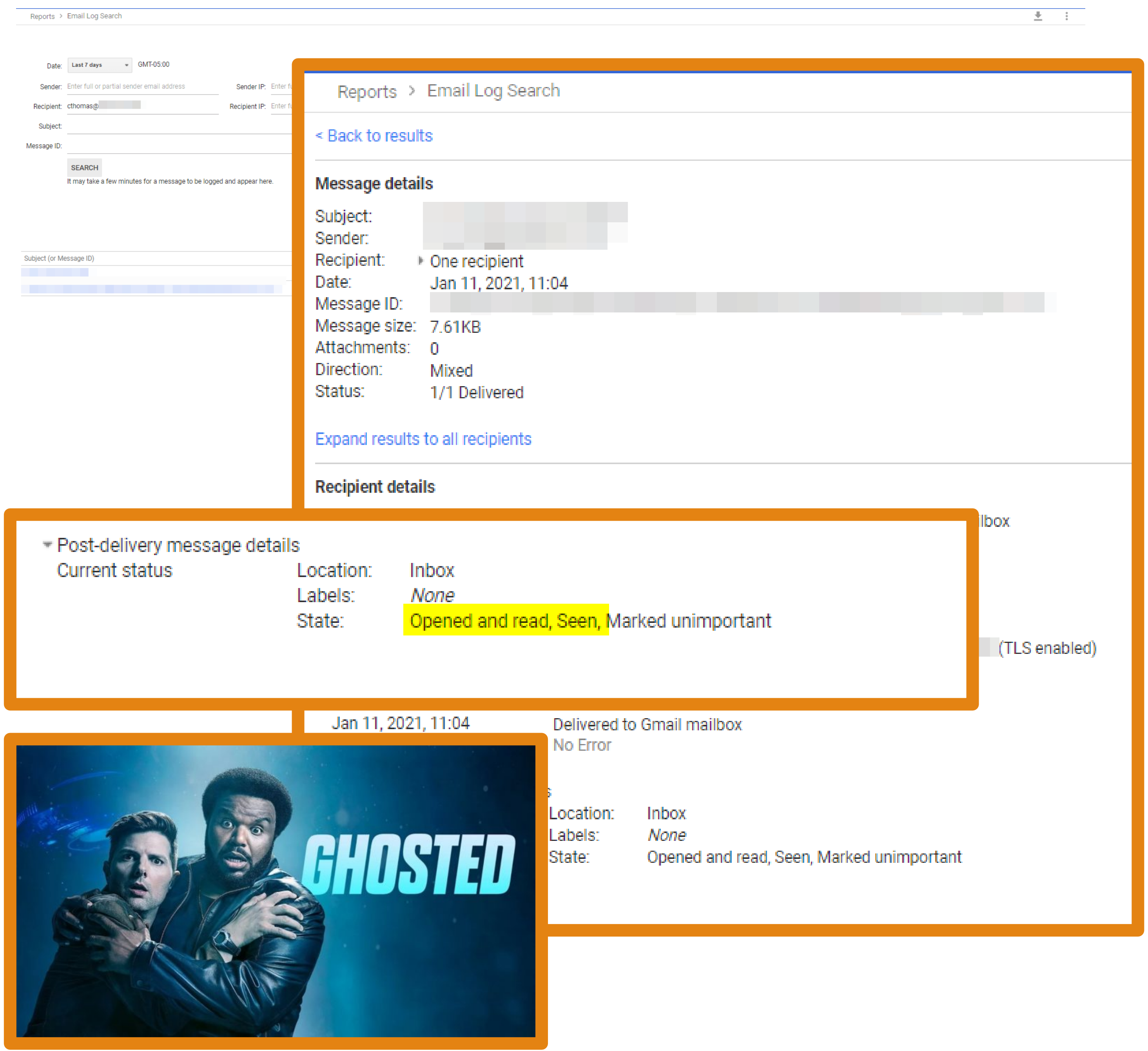
User creates ticket indicating that a student never replies to their email messages and wants to ensure the student is receiving the emails.

You find that the student is receiving the message …

… you open the message details to expand the recipient details …

… then you can see the state of the message …

… and introduce the user to the term 'ghosted' when you find the student replies to other teachers.



Reports › Email Log Search

Date: Last 7 days GMT-05:00

Sender: Enter full or partial sender email address

Sender IP: Enter f

Recipient: cthomas@[redacted]

Recipient IP: Enter f

Subject:

Message ID:

SEARCH

It may take a few minutes for a message to be logged and appear here.

Subject (or Message ID)

[redacted]

Reports › Email Log Search

< Back to results

Message details

Subject: [redacted]

Sender:

Recipient: One recipient

Date: Jan 11, 2021, 11:04

Message ID: [redacted]

Message size: 7.61KB

Attachments: 0

Direction: Mixed

Status: 1/1 Delivered

Expand results to all recipients

Recipient details

lbox

(TLS enabled)

Jan 11, 2021, 11:04 Delivered to Gmail mailbox

No Error

Location: Inbox

Labels: *None*

State: Opened and read, Seen, Marked unimportant

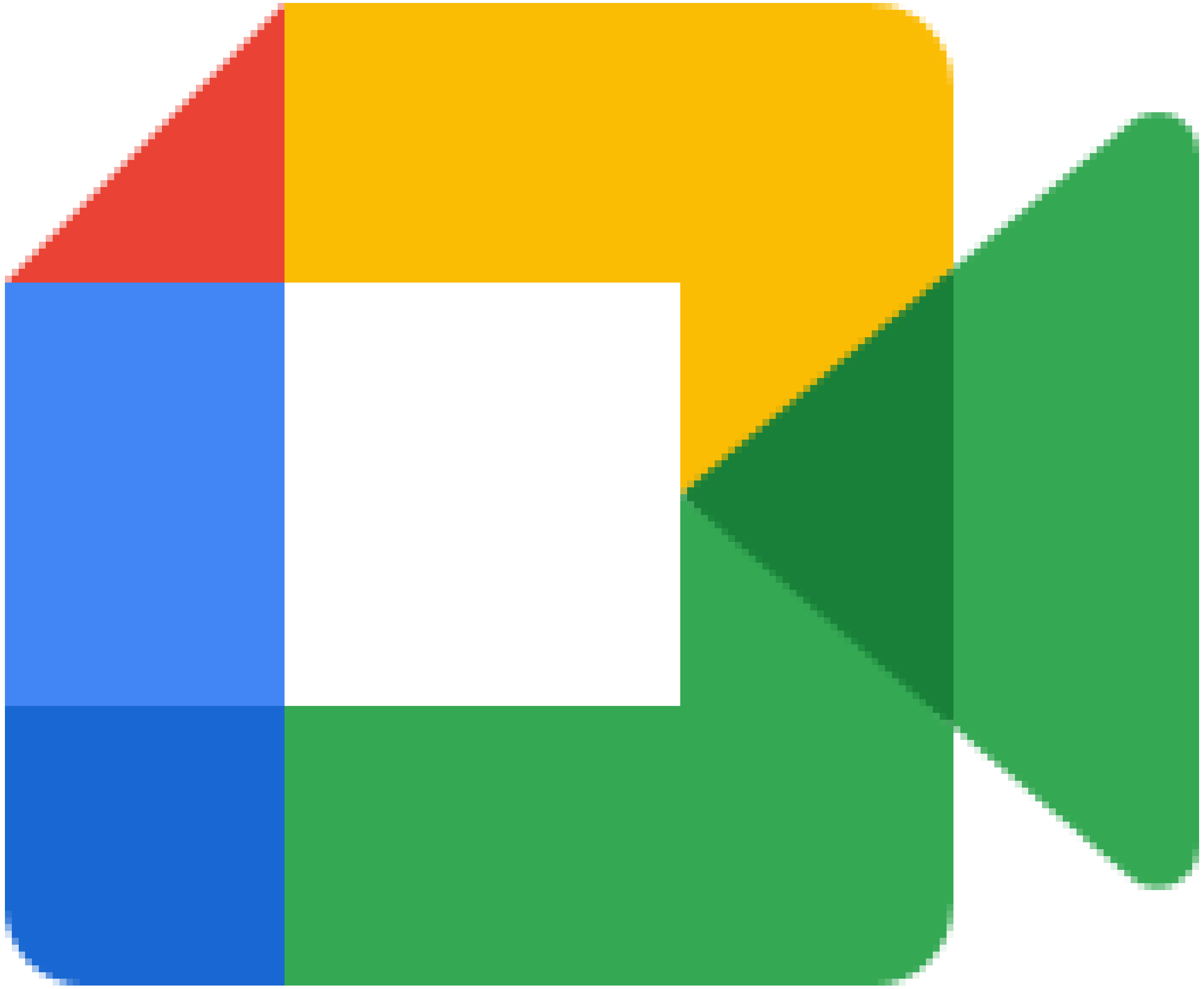
Post-delivery message details

Current status

Location: Inbox

Labels: *None*

State: Opened and read, Seen, Marked unimportant



Google Meet

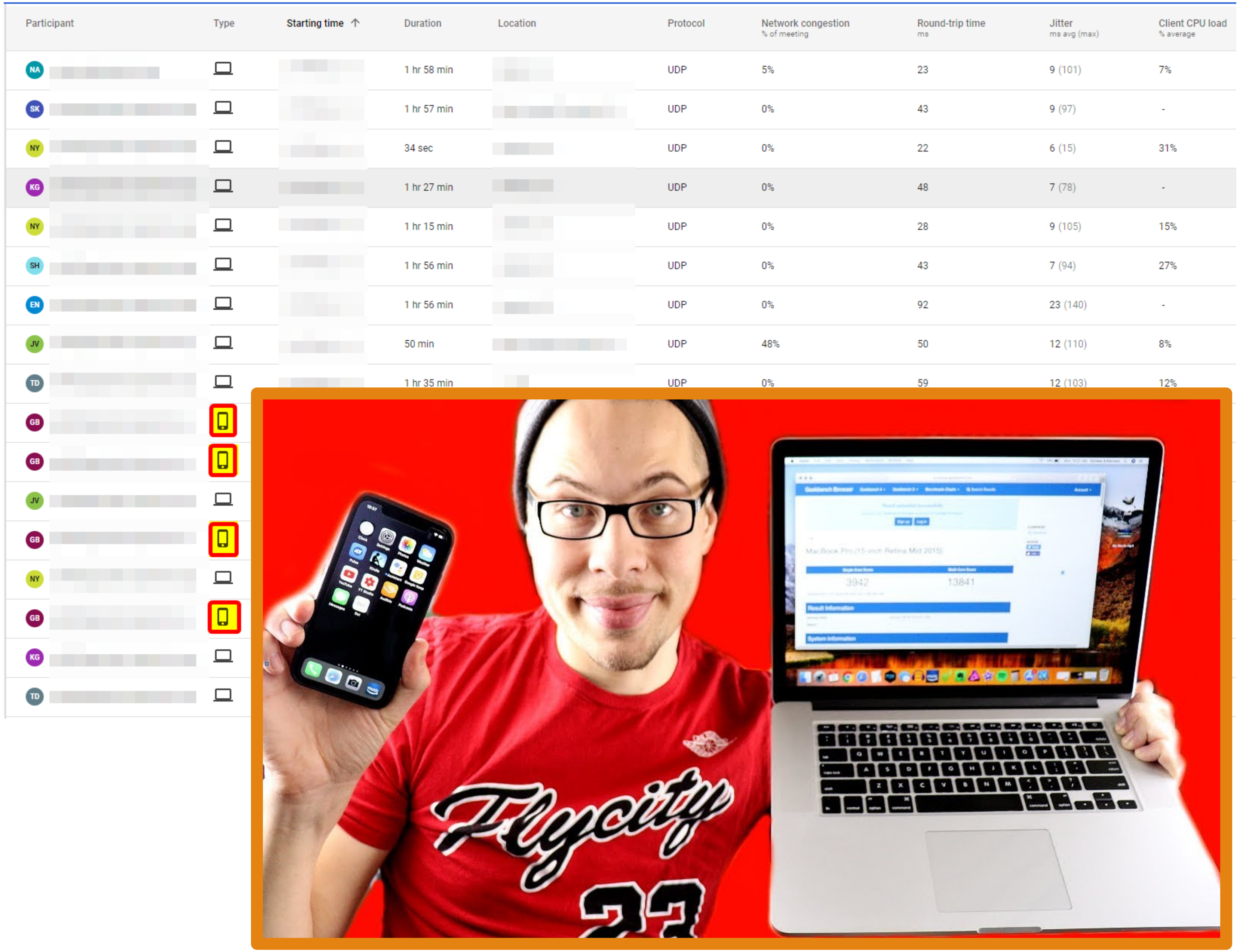
- Meet Quality Tool (https://meet.google.com/tools/quality/admin)
  - Connection speeds
  - Audio quality
  - Video quality
  - Join times
  - Exit times
  - Screen sharing logs
- We can't troubleshoot home networks, but we can advise things like asking family to consider limiting in-home streaming during class time to maximize available bandwidth for children learning.
- We can offer a replacement Chromebook to rule out hardware issues and verify the replacement device has Wi-Fi that is functional with school-provided Wi-Fi before sending it home.
- We can offer a school-provided MiFi as an alternative connection option, if any are available.

Google Meet Scenario

User creates ticket and indicates one student is having repeated Google Meet connection issues while the rest of the class does not appear impacted.

You find that this student is using an iOS mobile device to attend class through Google Meet …

… even though they were all supplied with a MacBook Pro. So, you request student use school-issued device and report if issues persist.



Participant	Type	Starting time ↑	Duration	Location	Protocol	Network congestion % of meeting	Round-trip time ms	Jitter ms avg (max)	Client CPU load % average
NA [redacted]	💻	[redacted]	1 hr 58 min	[redacted]	UDP	5%	23	9 (101)	7%
SK [redacted]	💻	[redacted]	1 hr 57 min	[redacted]	UDP	0%	43	9 (97)	-
NY [redacted]	💻	[redacted]	34 sec	[redacted]	UDP	0%	22	6 (15)	31%
KG [redacted]	💻	[redacted]	1 hr 27 min	[redacted]	UDP	0%	48	7 (78)	-
NY [redacted]	💻	[redacted]	1 hr 15 min	[redacted]	UDP	0%	28	9 (105)	15%
SH [redacted]	💻	[redacted]	1 hr 56 min	[redacted]	UDP	0%	43	7 (94)	27%
EN [redacted]	💻	[redacted]	1 hr 56 min	[redacted]	UDP	0%	92	23 (140)	-
JV [redacted]	💻	[redacted]	50 min	[redacted]	UDP	48%	50	12 (110)	8%
TD [redacted]	💻	[redacted]	1 hr 35 min	[redacted]	UDP	0%	59	12 (103)	12%
GB [redacted]	📱								
GB [redacted]	📱								
JV [redacted]	💻								
GB [redacted]	📱								
NY [redacted]	💻								
GB [redacted]	📱								
KG [redacted]	💻								
TD [redacted]	💻								

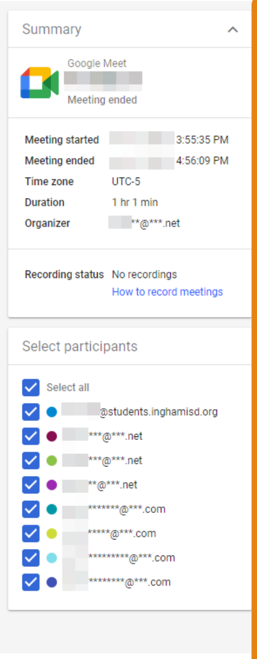
Google Meet External Domain Scenario

User creates ticket indicating that students' parents are noticing student in Google Meet during odd times.

You find that student is indeed joining Google Meet sessions hosted and attended by external users.

You are unable to determine who the host was as you were only provided 4 characters for the user name and only the domain ending.

You confirm that users can join any Google Meet, including consumer Gmail account Meet sessions and it doesn't appear you can prevent it.



Summary

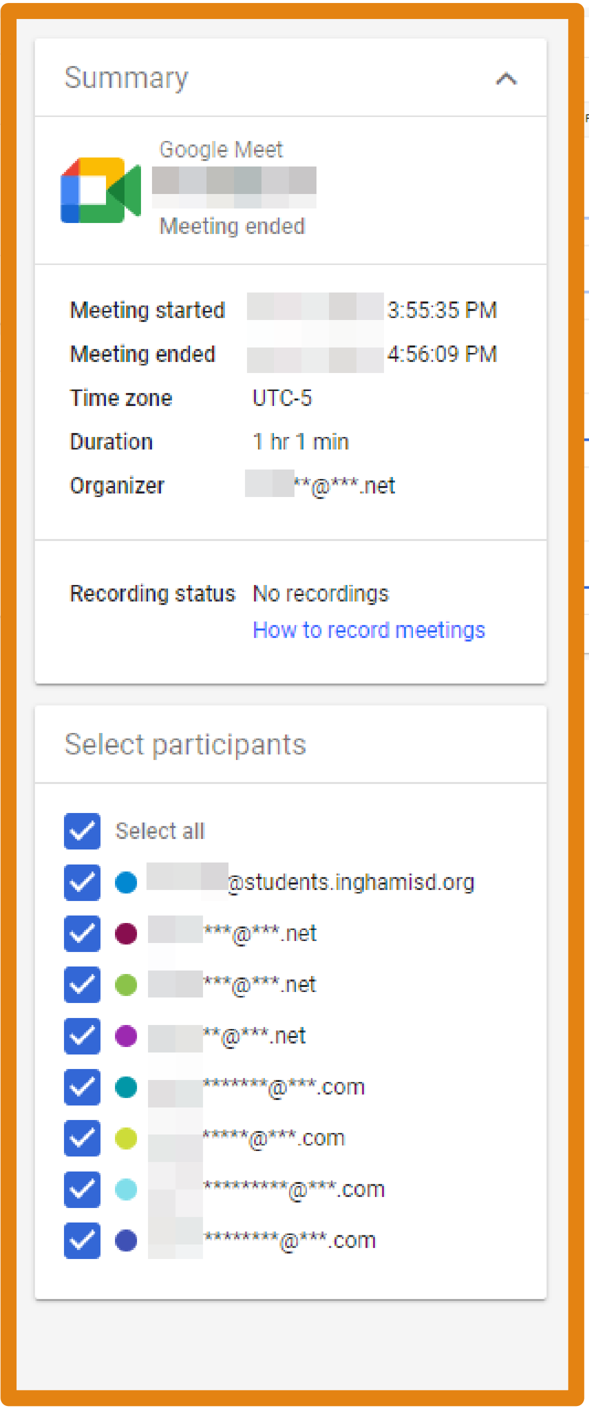
Google Meet
[redacted]
Meeting ended

Meeting started [redacted] 3:55:35 PM
Meeting ended [redacted] 4:56:09 PM
Time zone UTC-5
Duration 1 hr 1 min
Organizer [redacted]**@***.net

Recording status No recordings
How to record meetings

Select participants

☑ Select all
☑ ● [redacted]@students.inghamisd.org
☑ ● [redacted]***@***.net
☑ ● [redacted]***@***.net
☑ ● [redacted]**@***.net
☑ ● [redacted]*******@***.com
☑ ● [redacted]*****@***.com
☑ ● [redacted]*********@***.com
☑ ● [redacted]********@***.com



Summary

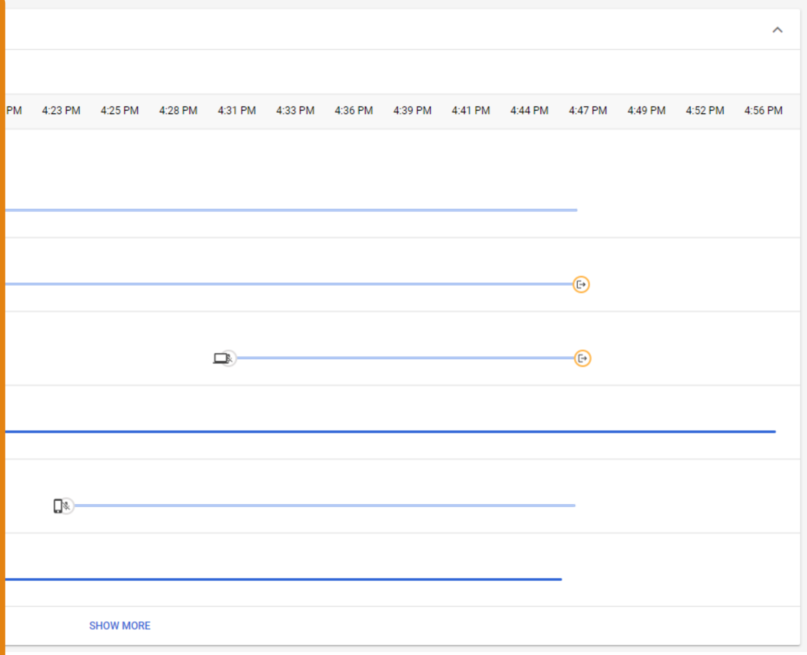
Google Meet
[redacted]
Meeting ended

Meeting started	[redacted] 3:55:35 PM
Meeting ended	[redacted] 4:56:09 PM
Time zone	UTC-5
Duration	1 hr 1 min
Organizer	[redacted]**@***.net

Recording status No recordings
How to record meetings

Select participants

☑ Select all
☑ ● [redacted]@students.inghamisd.org
☑ ● [redacted]***@***.net
☑ ● [redacted]***@***.net
☑ ● [redacted]**@***.net
☑ ● [redacted]*******@***.com
☑ ● [redacted]*****@***.com
☑ ● [redacted]*********@***.com
☑ ● [redacted]********@***.com



Incident Examples

- Colleague Changes Settings Without Informing The Team
- Colleague Changes Settings But You Forgot That They Informed The Team
- YOU Changed Settings But Forgot To Inform The Team
- Cyberbullying Between Students
- Self-Inflicted Cyberbullying For Attention
- Inappropriate Emails
- Unwanted Messages
- Profile Image Changing
- Student Runs Away

Recap & Q/A

- Learn to love logs.
- Consider all of the data sources when conducting your research.
  - Don’t assume you know where the user is communicating.
- Connect the dots to tell a narrative.