



D. STAFFORD
& ASSOCIATES

Title IX Investigator Technology and Investigations (Tier 6)

Presented by DSA Associates:

**Melissa McRae
Cathy Cocks
Adrienne Murray**

D. Stafford & Associates, LLC
179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
302-344-5809

Dolores@DStaffordandAssociates.com
www.dstaffordandassociates.com

©All rights reserved by DSA



Technology & Investigations

- Introductions
- Digital Evidence ("The What")
- Devices & Platforms ("The Where")
- Technical Investigations ("The How")
- Responsibilities, Challenges, Safety & Resilience

Adrienne Meador Murray, Vice President,
Equity Compliance and Civil Rights Services



In January 2014, Adrienne Meador Murray joined D. Stafford & Associates where she currently serves as the Vice President, Equity Compliance and Civil Rights Services after having been affiliated with D. Stafford & Associates as a part-time Associate since 2012 and the National Association of Clery Compliance Officers & Professionals (NACCOP) where she currently serves as Director of Training and Compliance Activities. Murray began her career in municipal law enforcement as a civilian employee with the City of Richmond Police Department (Virginia). She graduated from the Virginia Commonwealth University Police Training Academy and began her career as a sworn police officer for the University of Richmond (UR) Police Department (Virginia). At UR, Murray progressed through the ranks from a night shift patrol officer to Operations Lieutenant (overseeing criminal investigations, crime prevention and patrol) over the span of a decade before becoming the Chief of Police at Davidson

College in North Carolina. Most recently, Murray served as Chief of Police at Trinity Washington University (in Washington, D.C.).

As the Executive Director, Equity Compliance and Civil Rights Services for DSA, Murray builds on her 17-year career in law enforcement in which she became a nationally recognized expert in the field of best practice postsecondary institutional response to the sexual victimization of college women in the United States and in Canada. She is also a trained civil rights investigator and is well respected throughout the country for her ability to aid institutions in understating how to do best practice criminal and civil rights investigations concurrently. She is well known for her work in having provided support, advocacy and criminal investigative services for victims of sexual assault, stalking and intimate partner violence and is a sought-out speaker and investigator. She has expertise in the construction of best practice law enforcement standard operating procedures and training police officers to respond in best practice and trauma-informed ways to victims of sexual assault and intimate partner violence. In her current role, Murray coordinates curriculum development and instruction for national classes, including basic and advanced sexual misconduct investigation classes; an investigation of dating violence, domestic violence and stalking class; and a Title IX Coordinator/Investigator class offered through D. Stafford & Associates. To date, Murray has trained more than 3,500 criminal and civil rights investigators throughout the U.S.

Drawing on her experiences as a trained criminal and civil rights investigator, Murray also oversees independent investigations of complex sexual misconduct cases; conducts audits of Title IX/VAWA



P.O. Box 1121
Rehoboth Beach, DE 19971
Phone: (202) 438-5929
dolores@dstaffordandassociates.com

Compliance; drafts institutional sexual misconduct policies and procedures; and conducts campus-based trainings pertaining to the resolution of sexual misconduct offenses on college and university campuses. Murray frequently presents at regional and national conferences on topics such as the *Sexual Victimization of College Women*, *Understanding Consent and Incapacitation*, and *Responding to Sexual Assault on Campus: Clery Act and Title IX Implications*. Murray also conducts provincially specific sexual misconduct trainings throughout Canada.

Murray is a graduate of the University of Richmond, where she received her Bachelor's Degree in Applied Studies in Human Resource Management and of New England College, where she received her Master's Degree in Campus Public Safety Administration. Murray is also a graduate of the 235th session of the prestigious FBI National Academy where she was awarded a graduate certificate in Criminal Justice from the University of Virginia. She has authored numerous journal articles.



D. STAFFORD
& ASSOCIATES

P.O. Box 1121
Rehoboth Beach, DE 19971
Phone: (202) 438-5929

dolores@dstaffordandassociates.com

Catherine Cocks, M.A.
Consultant, Student Affairs, Title IX, and
Equity Compliance Services



Ms. Cocks has been a higher education professional for over thirty years. Her work with D. Stafford & Associates focuses on Title IX investigations and training; assessment of student affairs policies, practices and services; and behavioral threat assessment. Cathy was the Director of Community Standards for the University of Connecticut for 14 years where she managed the student conduct process, which included managing all Title IX cases involving student respondents and chaired the University's student threat assessment team. Prior to that, she held several positions within Residential Life at the University of Connecticut and Roger Williams University.

She is a faculty member for the Association for Student Conduct Administration's (ASCA) Donald D. Gehring Academy teaching on subjects such as ethics, governance, threat assessment, media relations, and higher education trends. She was an affiliated faculty

member for many years in the University of Connecticut's Higher Education and Student Affairs Master's program teaching "The Law, Ethics, and Decision-Making in Student Affairs."

Cathy has co-authored the "Philosophy of Student Conduct" chapter in the 2nd edition of "Student Conduct Practice" (2020) and was a member of the writing team for CAS Standards' Cross-functional Framework for Identifying and Responding to Behavioral Concerns.

Cathy is a Past President of ASCA. She has also served as a Circuit representative, co-chair of the Public Policy and Legislative Issues Committee, and as a member of the ASCA Expectations of Members Task Force. Cathy has served in a variety of leadership roles in NASPA Region I.

She was the 2015 recipient of ASCA's Donald D. Gehring Award. She is a past recipient of the NASPA Region I Mid-Level Student Affairs Professional Award and the NASPA Region I Continuous Service Award.

She earned her Master's degree in Higher Education Administration from the University of Connecticut and Bachelor's degree in Communications/Media from Fitchburg State University.



Melissa McRae, Project Associate



Melissa McRae is a retired Federal Bureau of Investigation (FBI) Supervisory Special Agent (SSA) known for building public and private sector partnerships, developing task forces, and coordinating complex international investigations with successful outcomes. During her career with the FBI, she specialized in investigating and overseeing National Security and Criminal computer intrusions, Internet Fraud, Insider Threats, and Theft of Trade Secrets. She led task forces in Richmond, Virginia addressing Cyber Crimes, Violent Crimes against Children, Civil Rights, and Hate Crime matters; as well as supervised Richmond's Computer Analysis Response Team (CART).

In 2015, Melissa was selected as the FBI's first permanent Cyber Assistant Legal Attaché (ALAT) in Canada, where she was responsible for collaborating with Canadian law enforcement and public sector partners and acting as the liaison for the FBI on cyber related investigations with a nexus in Canada. Through these partnerships, she coordinated international high profile Cyber investigations and enabled disruptions of major cyber threat groups impacting critical infrastructure and human safety across the world. As a result, Ms. McRae received the 2018 FBI Director's Award for International Excellence. Following her three-year assignment in Ottawa, Canada and prior to her retirement in 2019, Ms. McRae was the Special Advisor to the Operational Technology Division Deputy Assistant Directors. In this role, she provided guidance and assistance on critical and complex technological initiatives.

Melissa McRae has 28 years of experience in law enforcement and was a certified Defensive Tactics Instructor. Prior to her time in the FBI, she served as a Systems Administrator and Crime Analyst for the Hanover Sheriff's Office in Hanover, VA, where she transformed them from a paper base system to digital based Incident Base Reporting (IBR) system and co-chaired the Central Virginia Crime Analysis Network. Since retiring in 2019, she has served as volunteer in the Medical Reserve Corps, as an adjunct professor at Virginia Commonwealth University and as a Private Investigator.

She has a Bachelor's Degree from Virginia Tech University and participated in an Information Systems Post Baccalaureate Program from 1996 to 1998 at Virginia Commonwealth University. Melissa has received significant specialized training in Cyber Security, Incident Response, Investigations and Digital Forensics.

Over her law enforcement career, Melissa actively participated, created and led numerous working groups and programs providing awareness, training, and establishing information sharing platforms. This led to her receiving numerous accolades during her illustrious career, including: Incentive Award for outstanding contributions to the Operational Technology Division, 2019; FBI Director's Award for International



D. STAFFORD
& ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
Phone: (202) 438-5929
dolores@dstaffordandassociates.com

Excellence - AlphaBay/Hansa Investigation, 2018; Quality Step Increase Award for Richmond Cyber Crime Task Force Leadership, 2012; US Attorney Award, Eastern District of Virginia - Card Keeper Investigation, 2008; Quality Step Increase Award for Richmond's InfraGard Program Leadership, 2007; Recognition for Business Process Re-engineering (BPR) integrated Process Team work, 2006; Quality Step Increase Award for 9/11 CP Team Leadership & CT Intrusion Investigation, 2003; and Certificate of Achievement for development of North Texas Cyber Crimes Task Force, 2000.

INVESTIGATION CLASS ACRONYMS

- ASR:** Annual Security Report (often used as a reference to the Annual Security Report and/or the Annual Security and Fire Safety Report) that must be published by each institution of higher education.
- CSA:** Campus Security Authority—Individuals on each campus who have been identified by the Department of Education as persons who are required to report crimes that they become aware of to the Reporting Structure at each institution.
- DCL:** Dear Colleague Letter—this is a formal name of the method of communication from the Department of Education to college campuses. It is like naming their official “memo” to campuses.
- FERPA:** Family Educational Rights and Privacy Act—governs the confidentiality of student records.
- FNE:** Forensic Nurse Examiners
- GO:** General Order—some departments describe their operating procedures as general orders
- HEOA:** Higher Education Opportunity Act—the broader law that contains the Clery Act language and the fire safety and missing person language that is in the law but not contained within the “Clery Act” portion of the law.
- HIPAA:** Health Insurance and Privacy and Portability Act—governs privacy of medical records.
- MOU:** Memorandum of Understanding—an official agreement developed between agencies.
- NIBRS:** National Incident-Based Reporting System. 1 of 2 crime reporting systems developed by the FBI, but not the system that you are required to use for Clery Reporting—the only portion of this system that is used for Clery Act purposes are the 4 forcible and 2 non-forcible sex offense definitions.
- OCR:** Office of Civil Rights—the unit of the Department of Education that oversees Title IX Compliance.
- PD:** Police Department
- PS:** Public Safety
- PNG:** Persona-non-Grata—process used by some campuses not keep students from entering certain areas of the campus or the entire campus (administrative process) versus legal bar notice or trespass warning.
- SACC:** Sexual Assault Crisis Center, also known as Women’s Center.
- SANE:** Sexual Assault Nurse Examiner

SART: Sexual Assault Response Team

SOP: Standard Operating Procedures—some departments describe their operating procedures as Standard Operating Procedures. Some call them General Orders, etc...

SWA: Senior Women's Administrator (Athletics)

TWN: Timely Warning Notice

UCR: Uniformed Crime Report. This is 1 of 2 crime statistics reporting systems developed by the FBI. Institutions are required to use UCR Standards for counting and classifying crimes for reporting the Clery statistics.

VAWA: Violence Against Women Act



TITLE IX

Copyright

(Limited permission is granted to each attendee of this class to make training materials available per the requirements outlined in the Title IX Regulations published on May 19, 2020)

These materials are copyright of D. Stafford & Associates, LLC © 2025 D. STAFFORD & ASSOCIATES. All rights reserved.

Any distribution or reproduction of part or all of the contents in any form is prohibited other than the following:

- As required by 34 C.F.R. § 106.45(b)(1)(iii) and § 106.45(B)(10)(i)(D), this material in its entirety may be posted to the website of the institution in which you were associated with at the time in which you were enrolled in this training. D. Stafford & Associates gives permission for clients to convert the provided documents as necessary to be ADA-compliant.*
- Public inspection upon request.*

You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

No Recording or AI Usage Policy

Due to privacy concerns, intellectual property issues, and potential misuse of confidential information discussed during this session, attendees are strictly prohibited from recording this session or utilizing artificial intelligence (AI) tools like automatic transcription services or note-taking applications. Attendees found to be using such devices will be removed from the session and no refunds will be available.

ISSUANCE OF CERTIFICATES FOR COMPLETION

To receive a certificate, attendees must attend the majority of the class and have paid class invoice in full. This applies to both in-person classes and virtual classes. We understand that attendees may need to miss class for a legitimate reason for longer periods of time or may need to leave the room during a class for a few minutes to take a phone call or attend to other business. If an attendee misses a significant amount of the class (depending on the length of the class) or they miss an attendance poll, they will not be issued a certificate of completion for the class.

Attendees should report each absence using the online form provided (each class has its own unique form that is sent to all attendees via email prior to class). Attendees should complete the form twice for each absence: once to record their departure, and again to record their return. Attendees should complete the form immediately before leaving class and as soon as practicable upon their return. If an attendee signs out but does not sign back in, they will be marked absent for the remainder of the day.

The criteria for receiving a certificate is determined based on missed class time and participation in the Attendance Polls that will be launched throughout each day of class. Attendance polls are left up for approximately 5 minutes and the instructor notifies the attendees that a poll is being launched to ensure that everyone who is present can respond to the poll. If an attendee is unable to respond to the attendance poll, the attendee would need to **immediately post "I am here"** in the chat feature within the Zoom platform. That way we can give the attendee credit for being in attendance for that specific poll. Notifying us after the attendance poll has been closed will not allow us to give the attendee credit for being in class during the poll.

Some of our classes may qualify for credit toward a Master's Degree at New England College (and regardless if you decide to seek credit or not, accreditation requirements mandate that we follow the same standards for all class attendees), so we have strict attendance standards that we follow for issuance of a certificate. For DSA & NACCOP, issuance of a Certificate of Completion is verification of attendance.



TECHNOLOGY & INVESTIGATIONS



© 2025 D. STAFFORD & ASSOCIATES

1



A NOTE ON TRAINING



**This is not legal advice,
consult your lawyer!**

© 2025 D. STAFFORD & ASSOCIATES

2

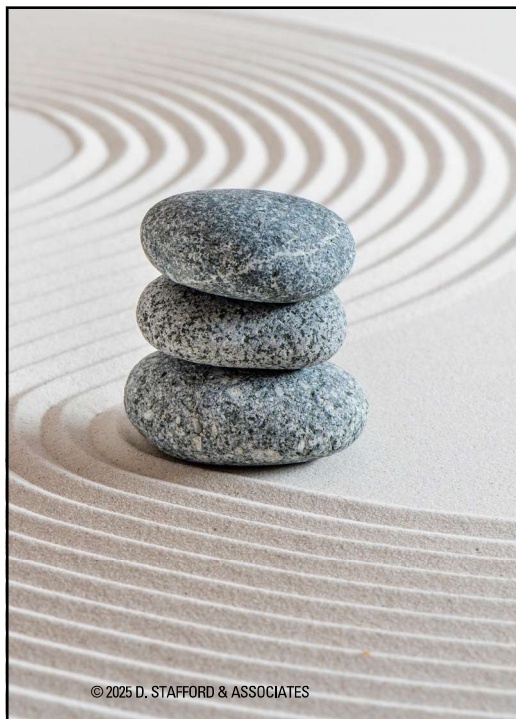
COPYRIGHT

(Limited permission is granted to each attendee of this class to make training materials available per the requirements outlined in the Title IX Regulations published on April 29, 2024)

These materials are copyright of D. Stafford & Associates, LLC

© 2025 D. STAFFORD & ASSOCIATES. All rights reserved.

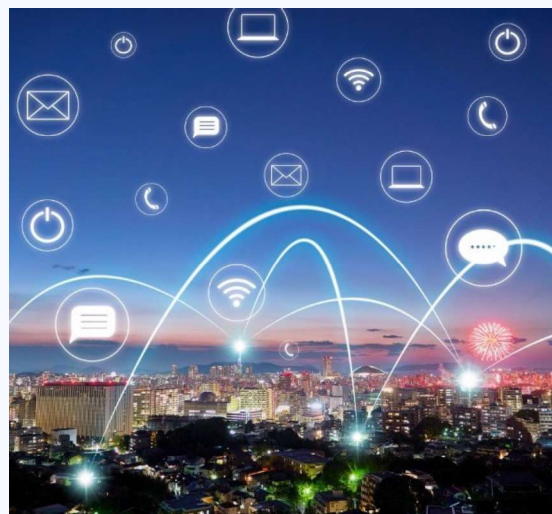
- Any distribution or reproduction of part or all of the contents in any form is prohibited other than the following:
 - As required by 34 C.F.R. § 106.8(f)(3), this material in its entirety may be made available upon request for inspection by members of the public in the presence of the Title IX Coordinator or their designee. This does not include providing copies as part of any request.
- **You may not post the materials on any website or provide copies of the materials.**
- You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any website or other form of electronic retrieval system.



AGENDA

- Introductions
 - Digital Footprints (“The What”)
 - Devices & Platforms (“The Where”)
 - Internet & Technical Investigations (“The How”)
 - Responsibilities, Challenges, Safety & Resilience
-

DIGITAL FOOTPRINTS "THE WHAT"



<https://www.youtube.com/watch?v=yrjT8m0hcKU>

DIGITAL FOOTPRINTS

Control
vs
No Control

Active
vs
Passive

DIGITAL FOOTPRINTS

Active (Yes Control)

- Comm
- Online
- Transac
- Upload
- (Photos
- Searches

Per Verizon,

“Cybercriminals today use a variety of strategies to access users’ online information; often, hackers gain access to users’ online profiles through information users share. For example, hackers might gain access to a user’s online bank account by answering their security questions with answers sourced from their digital footprint.”

HOW TO REDUCE DIGITAL FOOTPRINT

- Websites Visited & Actions Taken
- Search History

DIGITAL FOOTPRINTS

Content Transactional (non-content)

Stored Communications Act (“SCA”): 18 U.S.C. §§ 2701-2712

Law enforcement may obtain specific records about electronic communications of a subscriber or customer with an administrative, grand jury, or trial subpoena. Although the content of the electronic communications cannot be obtained, law enforcement may obtain:

name, address, records of sessions, including times and duration, local and long distance connection records, length of service and types of services utilized, telephone and instrument number or other subscriber number or identity, including any temporarily assigned network address, and the means and source of payment, including credit card or bank account number.

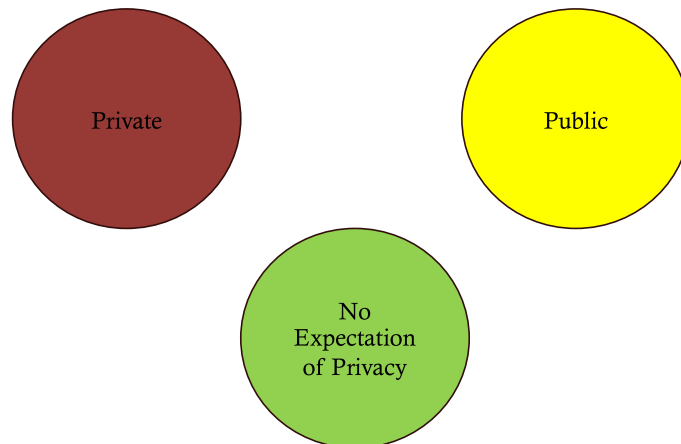
DIGITAL EVIDENCE “THE WHERE”



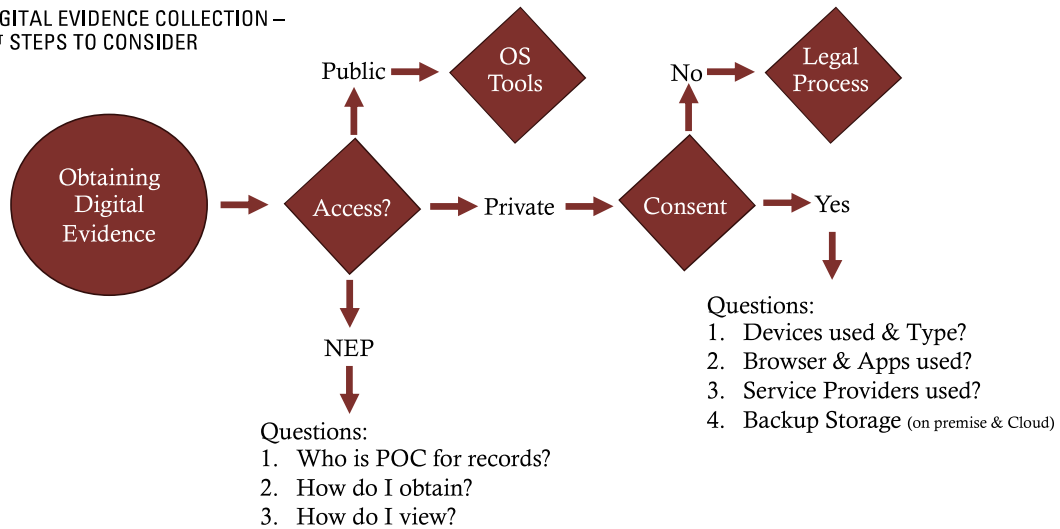
DIGITAL EVIDENCE



"THE WHERE" – LOCATION TYPE



DIGITAL EVIDENCE COLLECTION –
1ST STEPS TO CONSIDER



THE INTERNET

"DATA AT REST & IN MOTION"



INTERNET TERMS



Internet Service Provider (ISP)

Provides the internet to you (e.g., Xfinity)



Internet Protocol (IP) Address

ISP assigns device a unique number



Domain Name System (DNS)

Directory of server addresses



Router

Determine the best route for the code to take

INTERNET TERMS



Packets

File broken into many, many pieces



Transmission Control Protocol

Makes sure the packets arrive & puts them together



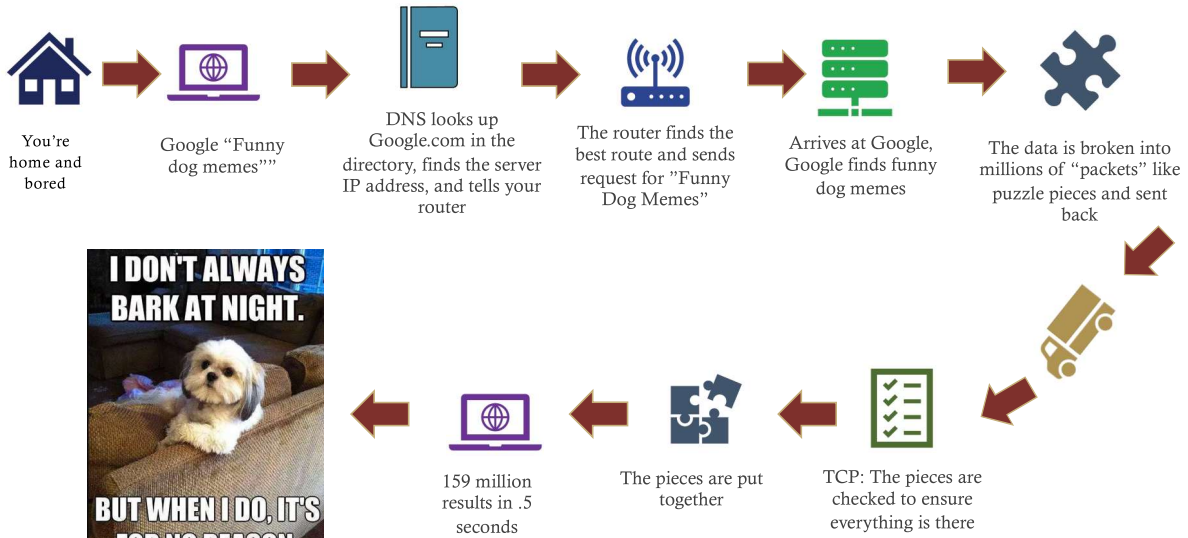
Cookies

Text files that contain identifying information stored in your browser by websites

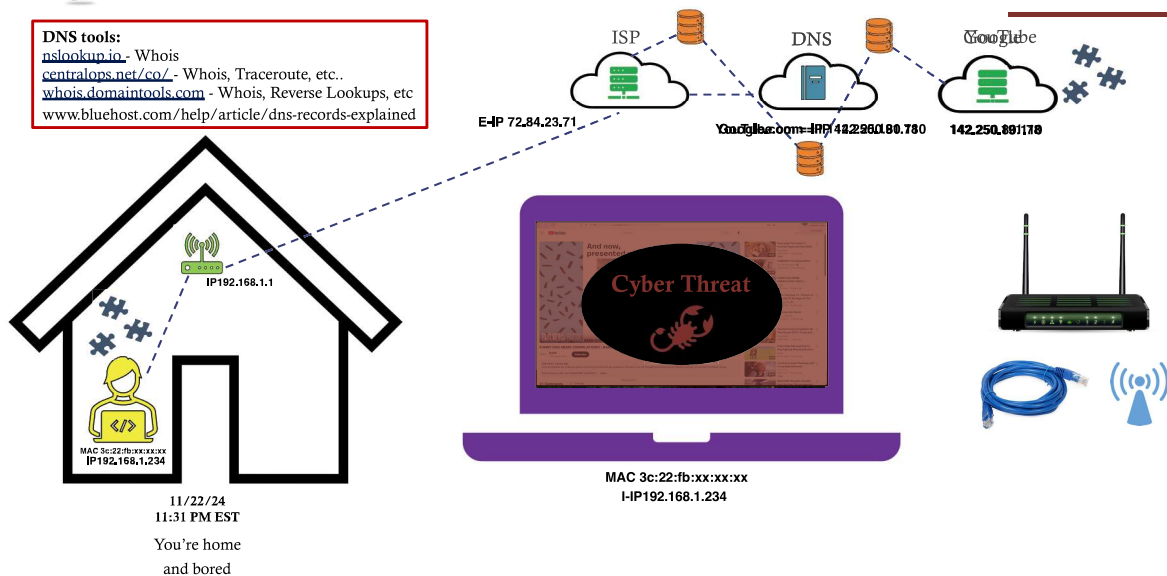


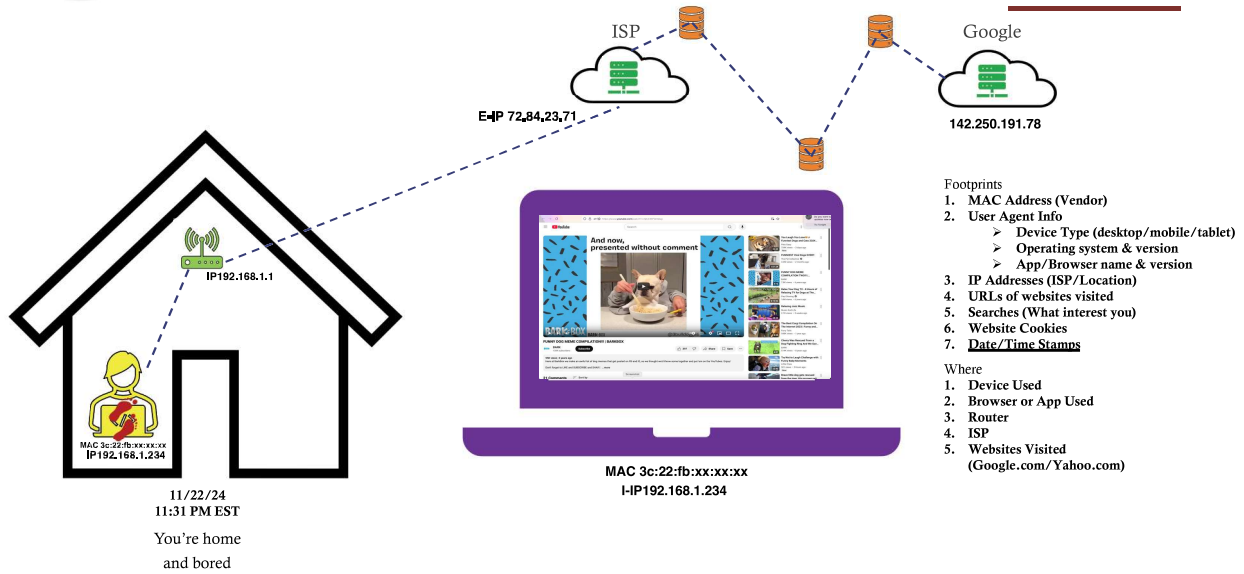
MAC Address

Unique serial number associated with the network interface of your computer



DNS tools:
nslookup.io - Whois
centralops.net/co/ - Whois, Traceroute, etc..
whois.domaintools.com - Whois, Reverse Lookups, etc
www.bluehost.com/help/article/dns-records-explained





TECHNICAL INVESTIGATIONS "THE HOW"



DEVICE:

Investigator's Notes (11/23/2024 11:15am EST)

- ✓ NEP/Consent/Legal Process
- ✓ Device1 Used: Apple Laptop
- ✓ Device1 Date/Time: 11/23/2024 11:20 am (EST)
- ✓ Device1 Info:
 - ✓ Type: Apple MacBook Pro Laptop
 - ✓ OS: Mac OS Sequoia Ver 15.0.1
 - ✓ Ser# M1SKSKSKS8B
 - ✓ Name: MacBook Pro
 - ✓ MAC Address: 3c:22:fb:xx:xx:xx
 - Rotating Wifi: 12:72:23:f0:e1:d9
- ✓ Apps on Device:
 - ✓ Browser(s): Safari & Firefox

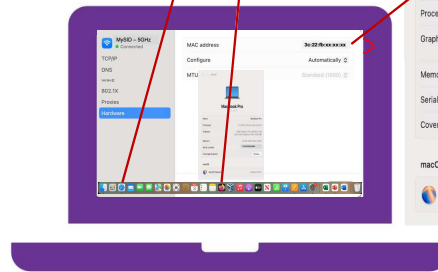
Private Wi-Fi address

Using a private address helps reduce tracking by Wi-Fi network operators. A rotating address reduces tracking on this network.

Rotating

Wi-Fi address

12:72:23:f0:e1:d9



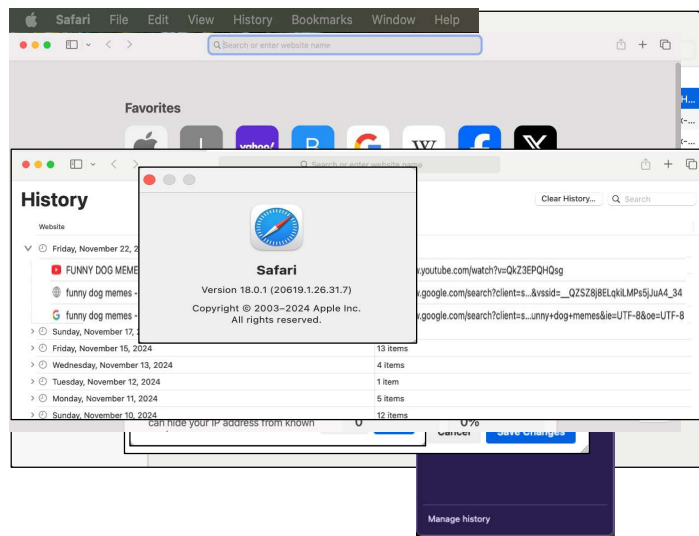
How to find MAC Address on Device:

<https://www.cmu.edu/computing/services/endpoint/network-access/mac-address.html>

APP/BROWSER:

Browsers History & Cookies:

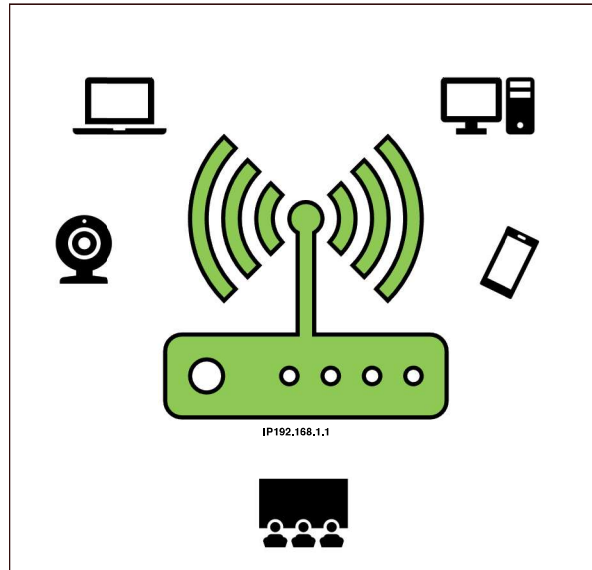
- ✓ Firefox:
 - ✓ History: Only history for today - Google search for "funny dog memes" & YouTube video "FUNNY DOG MEME COMPILATION!!! BARKBOX"
 - ✓ Cookies:
 - ✓ Above occurred 19 minutes ago
- ✓ Safari:
 - ✓ History: November 22, 2024 of same google search and YouTube video as above.
 - ✓ Current version 18.0.1
- ✓ Cache: Forensic team will review



ROUTER:

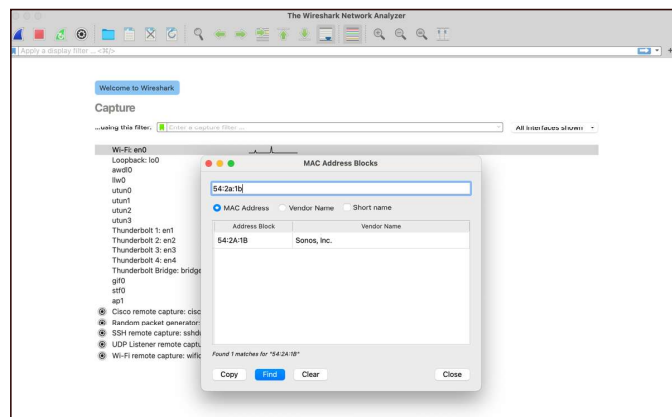
Router:

- ✓ Physical: Verizon FIOS Router Model#: G3100
 - ✓ Ser#: Gxxxxxx
 - ✓ WAN MAC: B9.F8.53.xx.xx.xx
 - ✓ Wi-Fi Name (SSID): FIOS (Default)
 - ✓ IP Internal: 192.168.1.1
 - ✓ IP External: 72.84.23.71
 - ✓ SSID(S): FIOS-WIFI5 & FIOS-WIFI2.4
 - ✓ Devices:
 - ✓ MacBook Pro 78:31:c1:e5:d4:73
 - ✓ MBP 64:4b:f0:13:br:ae
 - ✓ NEST1 f0:ef:86:f3:de:b3
- See attached for additional devices



MAC ADDRESSES

- 54:2a:1b:76:42:9a Sonos



Tools:

Application: Wireshark - <https://www.wireshark.org/>

Online Tools: MAC Address Lookup - <https://macvendorlookup.com/>

SERVICE PROVIDER:

1. Privacy Policy

- What is collected
- How used & shared
- Retention Period
- **Privacy Choices & Accessing Information**



Examples:

<https://www.directv.com/privacy/video-privacy-policy/>

<https://www.verizon.com/privacy/your-data>

<https://www.youtube.com/watch?v=3GV89k7c99g>



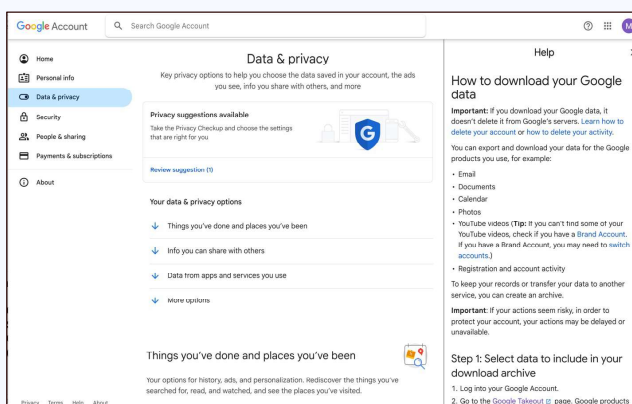
Download a portable copy of your information ↓

OTHER SERVICE PROVIDERS:

1. Telecommunication Services (e.g., AT&T)
2. Email Services (e.g., Google's Gmail)
3. Cloud Storage Services (e.g., iCloud)

Transactional
(non-content)

Content



Google Takeout Example

- Activities Accessed – IP, User Agent String, Service
- Access Logs – Device Info, User Given Name, Last Activity Date/Time

GOOGLE TAKEOUT:

Activity:

Search conducted at 2024-11-23 4:31:00 UTC

- ✓ - IP 72.84.23.71
- ✓ - User Agent String:
- ✓ App : SAFARI. Ver : 15.3.
- ✓ Os : MAC_OS. Ver : 10.15.6.
- ✓ Device Type : PC.

YouTube at 2024-11-23 4:32:01 UTC

- ✓ IP 72.84.23.71 (Same)
- ✓ User Agent String:
- ✓ App : YOUTUBE_APP. App Version : 17.07.2
- ✓ OS & Type same as above

Access Log:

- ✓ Apple PC iOS 10.15.7 named Macbook Pro
- Last Activity: 2024-11-23 4:34:37 UTC from US

© 2025 D. STAFFORD & ASSOCIATES

Activity Timestamp	IP Address	User Agent String	Product Name
2024-11-23 4:32:01 UTC	72.84.23.71	App : YOUTUBE_APP. App Version : 17.07.2. Os : MAC_OS. Os Version : 10.15.6. Device Type : PC. YouTube	Search
2024-11-23 4:31:00 UTC	72.84.23.71	App : SAFARI. App Version : 15.3. Os : MAC_OS. Os Version : 10.15.6. Device Type : PC.	Search



Device Type	Brand Name	Marketing Name	OS	OS Version	Device Model	User Given Name	Device Last Location
PC	Apple		iOS	10.15.7		Macbook Pro	CountryISO: US Last Activity Time: 2024-11-23 4:34:37 UTC

Online Tool:

Convert UTC to EST - <https://www.utctime.net/utc-to-est-converter>

27



MINI CASE STUDY #1 - COMPLAINANT

Julia reports to the Title IX investigator that she received an email on August 4th to her gmail.com account from bad_actor@gmail.com that was weird. The email stated, "Hey there remember me check out this video I found of you!" The email contained a link to webpage www.crazydays.com/6439_php987 and when she went to clicked on the link, she saw a YouTube video, posted of her. She suspects it may be Joe Doe from her economics class. While moving back into her dorm room, he texted her stating "Hey sexy, looking forward to seeing more of you this semester." As she never gave him her phone number and did not really know him, she thought that was creepy.

The video appeared to be of her in her res hall room last semester undressing and appears to have been taken from the window outside her room. She says she does not feel safe and wants you to expel him.

© 2025 D. STAFFORD & ASSOCIATES

28

EMAILS

[illegible]


Online Tools:

Reveal Email Headers: <https://support.google.com/mail/answer/29436?hl=en&siid=4335421611229011117-NA>

IPInfo - <https://ipinfo.io>

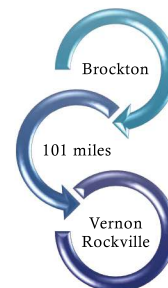
IP LOOKUP ACCURACY

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-5-1)

IP Address	Country	Region	City
12.34.56.789	United States of America 	Massachusetts	Brockton
ISP	Organization	Latitude	Longitude
Comcast Cable Communications LLC	Not Available	42.0834	-71.0184

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
12.34.56.789	United States 🇺🇸	Connecticut	Rockville
ISP	Organization	Latitude	Longitude
Comcast Cable Communications, LLC	Comcast IP Services, L.L.C. (comcast.com)	41.8668	-72.4495



EMAIL HEADERS – IP ORIGINATING FROM GOOGLE VS USER ISP

The image shows two side-by-side screenshots of email header analysis tools. The left tool displays headers for IP 209.85.220.41, with 'is_hosting: true' circled in red. The right tool displays headers for IP 2600:1003:b457:cdb:d89c:82f3:c0eb:2b20, with 'is_mobile: true' circled in red. Both tools show a list of IP addresses at the bottom: Your IP, 8.8.4.4, AS15169, 1.1.1.4, and AS451.

209.85.220.41

- postal: "94083",
- timezone: "America/Los_Angeles",
- is_anycast: false,
- is_mobile: false,
- is_anonymous: false,
- is_satellite: false,
- is_hosting: true,**
- asn: Object,

2600:1003:b457:cdb:d89c:82f3:c0eb:2b20

- timezone: "America/New_York",
- is_anycast: false,
- is_mobile: true,**
- is_anonymous: false,
- is_satellite: false,
- is_hosting: false,
- asn: Object,
- asn: "AS6167",

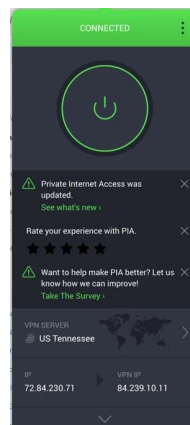
Download Original

Copy to clipboard

31

VIRTUAL PRIVATE NETWORK (VPN)

- Virtual Private Networks encrypt users' web traffic and mask their IP addresses
 - Many employers require a VPN if working from home, so your work is encrypted
- It prevents ISPs from tracking your browsing history
 - Be aware you may just be transferring the tracking to the VPN (<https://www.youtube.com/watch?v=3GV89k7c99g>)
- Challenges:
 - Man in the Middle Attacks (MITM)
 - Endpoint security
 - Backdoors
 - Compliance and regulatory requirements for content inspection



The image shows two side-by-side screenshots of IP header analysis tools. The left tool displays headers for IP 84.239.10.11, with 'vpn: true' circled in red. The right tool displays headers for IP 84.239.10.11, with 'type: "Business"' circled in red. Both tools show a list of IP addresses at the bottom: Your IP, 8.8.4.4, AS15169, 1.1.1.4, AS45194, and 68.87.41.40.

84.239.10.11

- ip: "84.239.10.11",
- city: "Atlanta",
- region: "Georgia",
- country: "US",
- loc: "33.7490,-84.3888",
- org: "AS212238 Datacamp Limited",
- postal: "30302",
- timezone: "America/New_York",
- asn: Object,
- vpn: true,**
- type: "Business",
- tor: false,
- relay: false,
- hosting: true,
- service: "",


84.239.10.11

- type: "Business",
- vpn: true,
- tor: false,
- relay: false,
- hosting: true,
- service: "",

32

EMAIL HEADER EXERCISE

From: Microsoft <Microsoft-noreply@microsoft.com>
Date: Mon, 09 Dec 2024 at 6:00 PM
Subject: Your Microsoft order on December 9, 2024
To: <stafford@staffordandassociates.com>



Review details of your Microsoft order

Thanks for your order on August 16, 2024.

You can manage your subscriptions in the Microsoft 365 admin center.

[Go to Microsoft 365 admin center >](#)

Billing information Order Id

Support Helpline : 1-(805) 316-0078 ef1e6ee8-0480-494d-d07a-a75dfc39ca47

Billing profile:
1 Microsoft Way
Redmond, wa, 98052-8300

Cloud	Your order items	Quantity	Unit price	Price
Global	Microsoft 365 Business Premium	1	\$792.00 USD	\$873.58 USD

Subtotal **\$873.58 USD**

Subtotal does not include any applicable taxes or fees except where specifically displayed on the invoice.
Please see your invoice for the final amount.



Assignment:

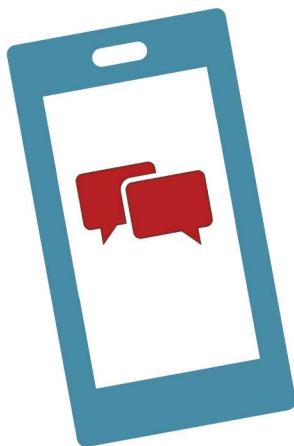
A friend receives an email from Microsoft-noreply@microsoft.com regarding a Microsoft order for Microsoft 365. He asks if you think it is legit.

What would be your first question?

What might you ask him to send you?

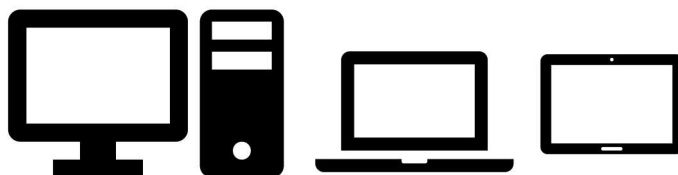
What actions would you take to determine if this email was fraudulent?

TEXT



Questions?

1. Device Used
2. [App Used](#)
3. [Collection Method](#)





POPULAR GROUP MESSAGING APPS



Phone App

- Messaging app that comes with the phone
- Examples:
 - Apple iMessage
 - Messages by Google
 - Samsung Messages
- End-to-end encryption is typical

GroupMe

- Owned by Microsoft
- Syncs with contacts
- User can make groups up to 500 people
- Does not have end-to-end encryption

WhatsApp

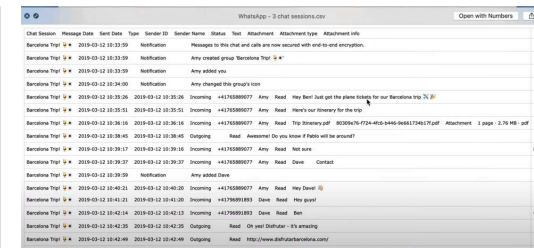
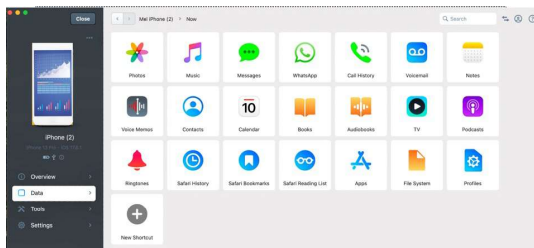
- Owned by Facebook
- WhatsApp does not retain messages once they are delivered
- End-to-end encryption does not allow WhatsApp to see the content

<https://www.cnbc.com/2024/12/15/why-the-fbi-wants-you-to-use-end-to-end-encrypted-messaging.html>

COLLECTION TECHNIQUES



1. Manual (Screen Shots)
2. Provider or Cloud Backup (if applicable)
3. Extraction Tool (e.g. iMazing for Apple Devices, Droid Transfer or SMS Backup+)



<https://www.youtube.com/watch?v=FHZc04xCa0>

iMazing export to csv

THE LEAK

Cyber Threat



You are investigating a dating violence case. You have just spoken to the complainant. The complainant is concerned because she is getting text messages from an unknown number that indicate the sender knows what the complainant has been sharing with you through email. For example, one text referred to photos that she had sent to you. Another text asked her what she was doing after a scheduled meeting with you. She is afraid someone is sharing information with the respondent.

All the case information is maintained in a case database system. The only people who have access to the information are the Title IX Coordinator and the other five investigators.

What would you do?

';--have i been pwned?

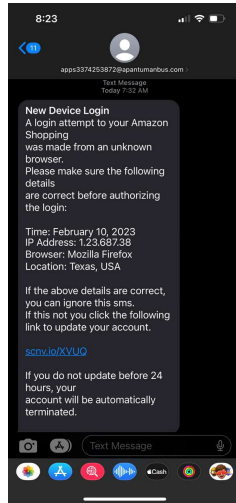
Check if your email or phone is in a data breach

Multi-Factor Authentication (MFA)



MESSAGES EXERCISE

Real or Fake?



Google has locked your gmail account, melissa@gmail.com, due to multiple attempts to log in to account with an incorrect password. Learn more at [google.com](https://www.google.com).



Spoof Messages

<https://www.youtube.com/watch?v=uJBZd2Ztglc>

Creating Fake Msg (ios8text.com)

<https://www.youtube.com/watch?v=E1qcOpUJEXec>

Deepfake Scams "World of AI"



COMMUNICATIONS – INVESTIGATOR CHALLENGES



Terms - <https://www.urbandictionary.com>



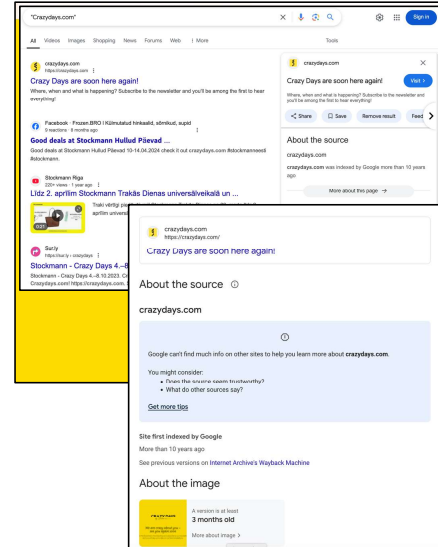
Sexual Emojis - <https://gabb.com/blog/sexual-emojis/>

WEBSITE

www.crazydays.com/6439_php987

1. Was this the actual URL or has true URL been masked or altered?
2. Does URL show up in complainant's web history?
3. What does domain registration reveal?
www.domain.com/whois/whois
nslookup.io
centralops.net/co/
whois.domaintools.com
4. What does a search of the domain reveal?
Google.com, Duckduckgo.com, bing.com, etc...
(Try multiple)
5. Is there a screen capture on the Internet Archive?
<https://web.archive.org/>

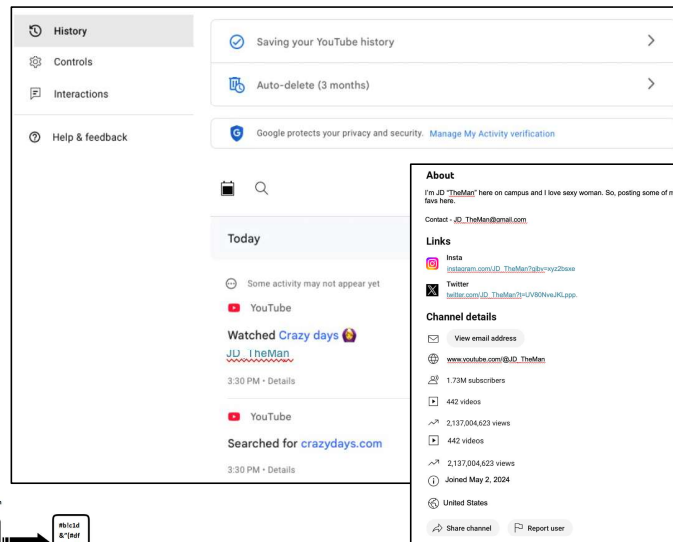
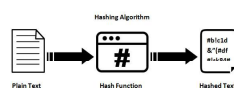
Domain Name: crazydays.com
Registry Domain ID: 42287159_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2024-11-09T01:11:07Z
Creation Date: 2005-11-13T04:58:23Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1 8887807723
Domain Status: clientTransferProhibited http://www.icann.org/esp/clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Stockmann Oyj Abp
Registrant Street: Aleksanterinkatu 52 B
Registrant City: Helsinki
Registrant State/Province:
Registrant Postal Code: 00100
Registrant Country: FI
Registrant Phone: +358.91211
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domains@stockmann.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Stockmann Oyj Abp
Admin Street: Aleksanterinkatu 52 B
Admin City: Helsinki
Admin State/Province:
Admin Postal Code: 00100
Admin Country: FI
Admin Phone: +358.91211



YOUTUBE

The Video

1. What does complainant's Browser History or Google/YouTube History reveal?
2. If YouTube History reveals the alleged video, does it associate it to a YouTube Profile?
3. What information can you obtain from YouTube Profile?
 - Other accounts
 - Location
 - Contact information
4. Can video be taken down?
 - <https://support.google.com/websearch/troubleshooter/3111061?hl=en>
5. What if video was also on JD_TheMan's Instagram site?
 - <https://help.instagram.com/>
 - <https://cybercivilrights.org/ccri-safety-center/#online-removal>
 - <https://stopncii.org/>





© 2025 D. STAFFORD & ASSOCIATES

MINI CASE STUDY #1 - RESPONDENT

After collecting pertinent information from complainant, the Title IX investigator takes next steps to identify respondent and collect other pertinent evidence to help decision makers determine if policy violation occurred:

1. Institution Logs & Records Review (NEP)
2. OSINT (Public)
3. Respondent Interview & Device Review (Private/Consent)

43



OPEN-SOURCE INTELLIGENCE

1. Database & On-line Resources
2. Internet Searches
 - Search Engines
 - Boolean Searches
3. Social Media Searches
 - Manual Digging
 - [OSINT Framework](#)

* Recommend using a [Virtual Machine](#)



© 2025 D. STAFFORD & ASSOCIATES

44

OSINT DATABASE & ON-LINE RESOURCES



People Search
Engines



Court Records

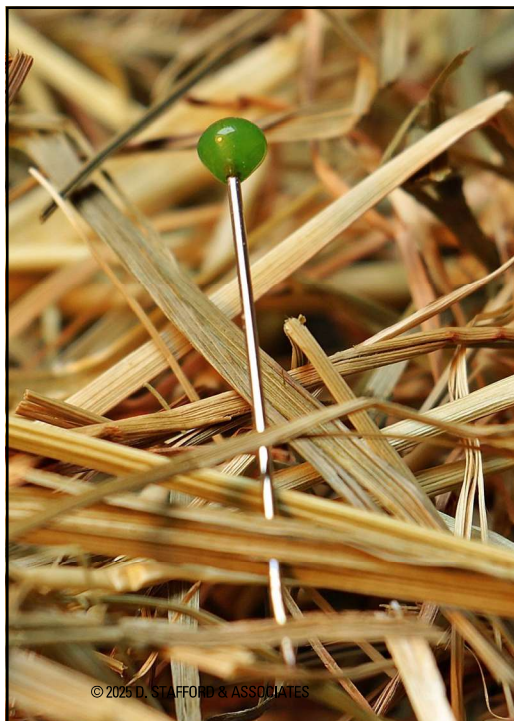


Property Records



Vehicle Records

- Sex Offender Registries
- Court Records
- Freedom of Information Act (FOIA) Rights and Responsibilities



SEARCH ENGINES

- Search engines like Google can be like finding a pot of gold...or a needle in a haystack.
- The right combination of terms, phrases, and creativity is the key to an effective search.

BOOLEAN

General:
Apple watch

- 2,380,000,000 results

And/or:
Apple and watch
not fruit

- 119,000,000 results

Site specific:
"Apple Watch"
site:reddit.com

- 950,000 results all on Reddit

USERNAMES



Most people use the same username across their accounts and often it is the first part of their email address



Some college admissions applications ask for usernames



People like to use birthdates, jersey numbers from sports

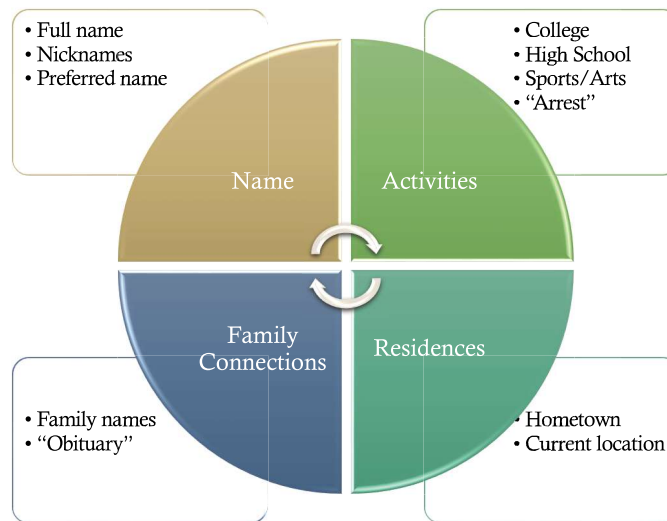


Witnesses know usernames!

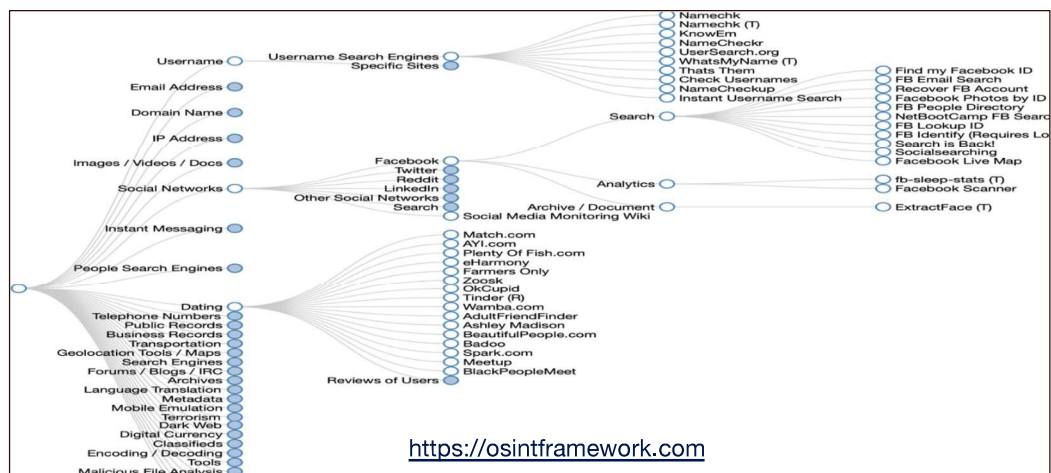


Instead of
FirstName
LastName, more
are using
FirstName
MiddleName

SEARCH TERMS

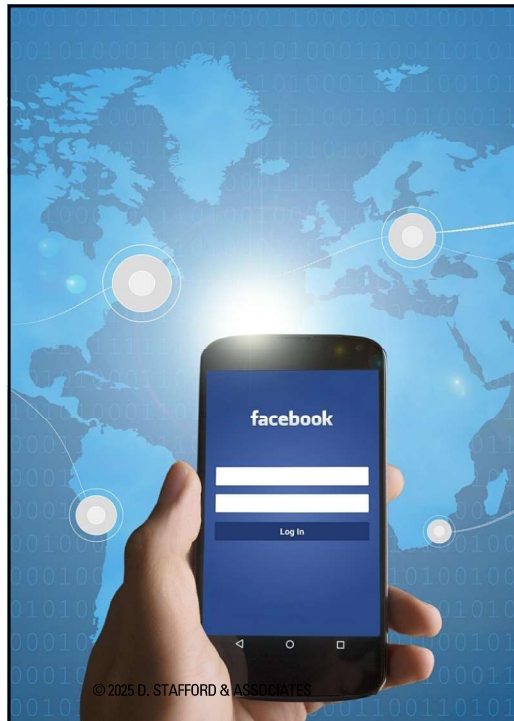


OPEN-SOURCE INTELLIGENCE (OSINT)



SOCIAL MEDIA SEARCHES

- Wealth of Information
 - Relationships
 - Locations
 - Activities & Dates
 - Images & more
- Search Technique “Creativity is the key”
- Challenges & Security



© 2025 D. STAFFORD & ASSOCIATES

51

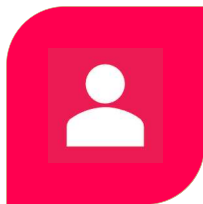
SOCIAL MEDIA PLATFORMS



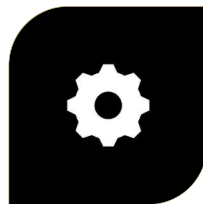
© 2025 D. STAFFORD & ASSOCIATES

52

FEATURES



Functions



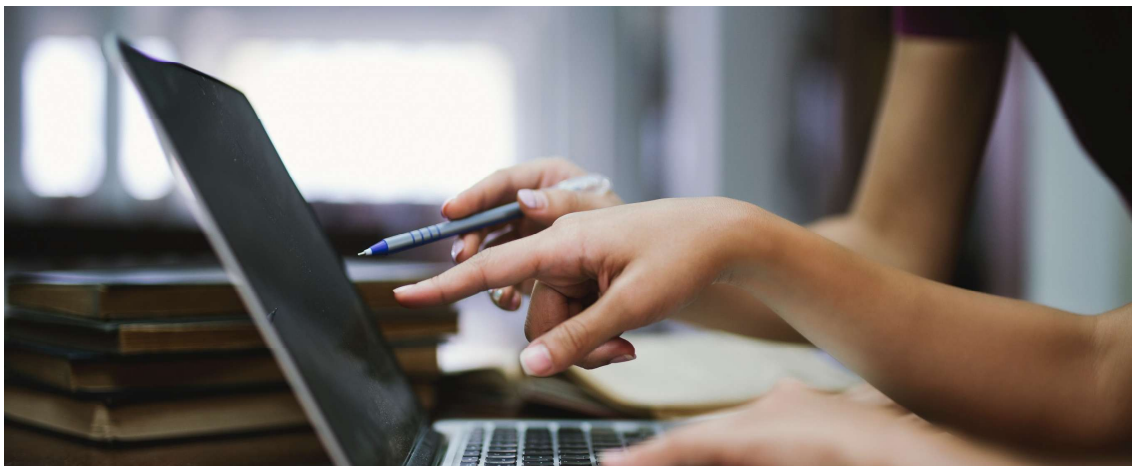
Default Settings



Obtaining Records
(Retention)

<https://www.facebook.com/help>
Popular Social Media & Dating Site Examples

SNAPCHAT CASE EXAMPLE



Criminal Complaint - <https://www.justice.gov/usao-dc/case-multi-defendant/file/1434576/dj>

SOCIAL MEDIA DISCUSSION



Take a few minutes and think about one of your cases involving social media.

1. What site was used?
2. How was it used?
3. What type of features does the site possess?
4. What digital evidence do they maintain?
5. What is the privacy policy? What could you collect and how? Do they allow for download of owner data?

Example: YikYak



MINI CASE STUDY #1 - RESPONDENT

After collecting pertinent information from complainant, the Title IX investigator takes next steps to identify respondent and collect other pertinent evidence to help decision makers determine if policy violation occurred:

1. Institution Logs & Records Review (NEP)
2. OSINT (Public)
3. Respondent Interview & Device Review (Private/Consent)

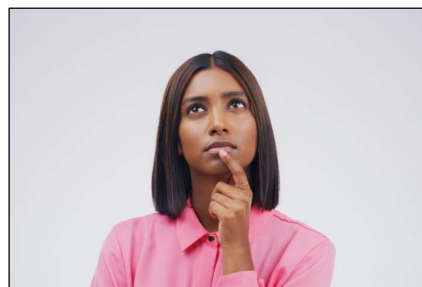
HOW CAN DIGITAL EVIDENCE HELP IN TITLE IX CASES?

1. Timeline of Events
2. Corroborating or Disputing Claims
3. Demonstrating Consent or Lack Thereof
4. Confirmation of Locations
5. Patterns of Behavior
6. Supporting Due Process



THINGS TO CONSIDER

1. Multi-User Access
2. Institutional Policy (Collection/Use)
3. Privacy & Ethical Concerns
4. Authenticity & Integrity



Note: Technical expertise to confirm authenticity, check for accuracy and completeness, and place findings in the correct investigative context.

5. Legal Counsel Consultation

CLOSING THOUGHTS

1. Use Reliable Sources & Stay Aware
2. Ensure Accuracy of Timelines
3. Validate, Validate, Validate
4. Be Persistent
5. Do Your Due Diligence



OTHER D. STAFFORD TRAINING OPPORTUNITIES

Title IX Coordinator Track

- ☐ Tier 1: Law and Policy
- ☐ Tier 2: Sex Discrimination Response
- ☐ Tier 3: Safety & Risk Analyses for Sex-Based Harassment Emergency Removals

Investigator Track

- ☐ Tier 1: Sex-Based Harassment Investigations
- ☐ Tier 2: Dating/Domestic Violence and Stalking (DVDVS) Investigations
- ☐ Tier 3: Case Study and Simulation (Interviewing)
- ☐ Tier 4: Statement Analysis
- ☐ Tier 5: Report Writing
- ☒ Tier 6: Technology & Investigations
- ☐ Tier 7: Violence Against Men

Related Offerings

- ☐ Institutional trainings
- ☐ Threat Assessment Teams
- ☐ Clery Compliance
- ☐ Procedural Justice
- ☐ Appellate Officer (www.naccop.org)
- ☐ Constructing Resolution Processes (www.naccop.org)
- ☐ Title IX Webinars (www.naccop.org)



THANK YOU



POPULAR SOCIAL MEDIA & DATING APP FEATURES:

1. [TikTok](https://tiktok.com/feedback)
(tiktok.com/feedback)
2. [Snapchat](https://support.snapchat.com)
(support.snapchat.com)
3. [Instagram](https://help.instagram.com)
(help.instagram.com)
4. [Facebook](https://facebook.com/help)
(facebook.com/help)
5. [Tinder/Grinder](https://help.tinder.com)
(help.tinder.com; help.grindr.com)

* Caveat: Students should validate if features have changed



TIKTOK FEATURES



Browse without an account



Need an account to post



Default setting is "Public"



TIKTOK & INVESTIGATIONS

- Users can download all their data
- Users can report problematic behavior
- Users can block other users and allow others to download their videos
- Comments are saved with the videos



TIKTOK & LAW ENFORCEMENT

- “TikTok may hold the following user data, which can be the subject of a valid law enforcement request:
 - Subscriber Information [TikTok username, Email address (depending on user’s sign-up method), Phone number (depending on user’s sign-up method), Account creation date, IP address at account creation, Device information]
 - Log-in/log-out data [IP address of account login/logouts]
 - Interaction data (non-content) [IP address logs for interactions (for a specified period only), Video creation time/date]
 - Content data [Video content, Comments, Direct message content]”

SNAPCHAT FEATURES

* Caveat: Students should validate if features have changed



Username
and vanity
name



Upload
contacts or
search for
friends



Snap



Chat



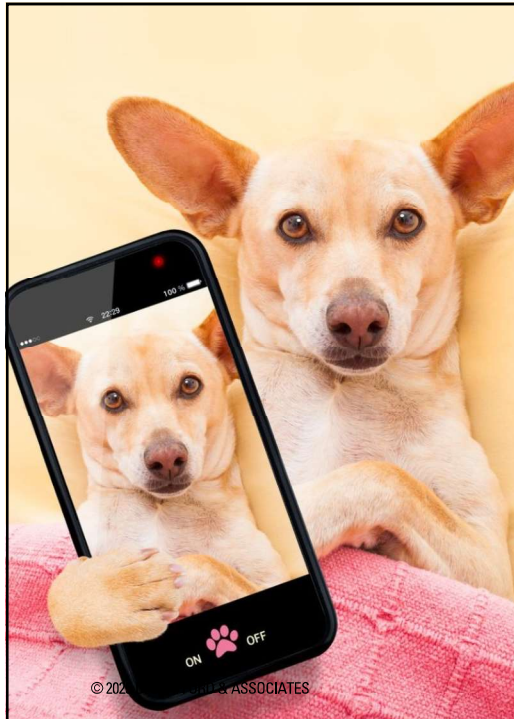
Stories



Snap map



Memories



ABOUT SNAPCHAT

- Snapchat is enjoying increasing popularity with 18 to 24-year olds
- Snapchat was first known for the increased popularity in sexting (sending sexually explicit media)
- Posts are recent and therefore, more timely
- Part of its popularity is the immediate deletion of the posts (more on this later)

69

STORIES

Private Stories

- Only the user can add Snaps to their Private Story and they can choose which friends can view the story. Only friends with access to the Private Story are notified when something is added.

Custom Stories

- Custom Stories are for the user and their friends. The user and their friends can view and add Snaps to a Custom Story.

Geo Stories

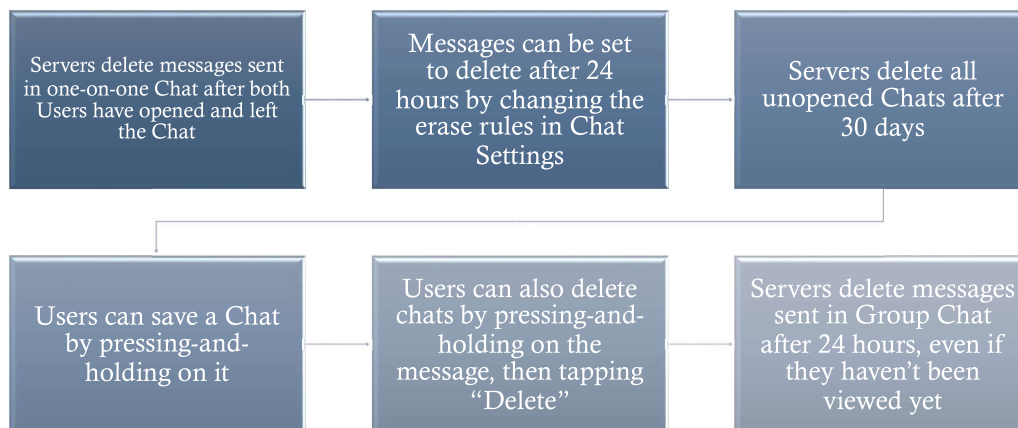
- Geo Stories are for the user and nearby Snapchatters. Snapchatters must be near the location the User chooses to view and add to the Story.
- Other Snapchatter's who are a part of that Story will know the user's location.

SNAPCHAT DELETION PROCEDURES - SNAPS



support.snapchat.com

SNAPCHAT DELETION PROCEDURES - CHATS



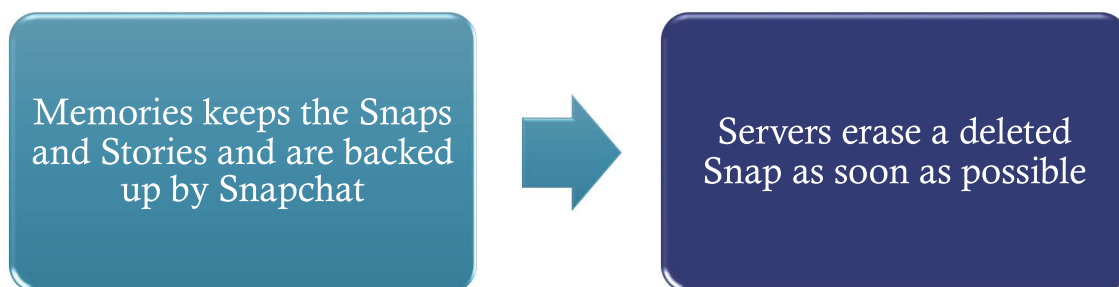
support.snapchat.com

SNAPCHAT DELETION PROCEDURES - STORIES



support.snapchat.com

SNAPCHAT DELETION PROCEDURES - MEMORIES



support.snapchat.com



© 2025 D. STAFFORD & ASSOCIATES

SNAPCHAT & INVESTIGATIONS

- Often, you have nothing except for what people say they sent/received
- Do not ask someone to “screenshot” an image because the sender is sent a notification - use another phone to take a photo of the screen

75



SNAPCHAT & LAW ENFORCEMENT

- Before sending a legal request, law enforcement must know the username (not the vanity name).
- Snapchat has policies allowing for preservation and emergency requests.
- A handbook is available on Snapchat’s website.
- Be aware of the deletion timeline so requests can be submitted prior to deletion.

support.snapchat.com

© 2025 D. STAFFORD & ASSOCIATES

76

INSTAGRAM FEATURES



Different names
for real and
“finsta”
accounts



Upload photos,
use filters



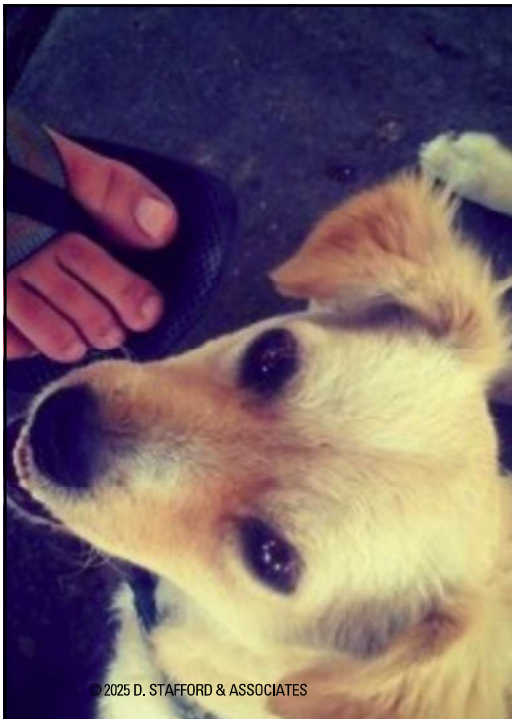
Story
(disappears after
24 hours)



“Like” and
comment



Direct message



ABOUT INSTAGRAM

- Launched in 2010 with this photo of a dog
- Within two months of its launch, Instagram had 1 million registered users
- It now has more than 1 billion users
- A means to chronicle life events – big and small
- Curates an “image” or “brand” of a person
- Owned by Facebook

"FINSTA"

- Users have a second account beyond their "Real" account.
- The "Real" account shows a carefully created life of friends, looks, and leading a great life (account parents/family see).
- "Finsta" is the account for friends.
 - Uses a name not known to parents and a different email or phone number so it can't be connected
 - Displays more of "real life" – imperfect photos, struggles, memes, etc.



INSTAGRAM & INVESTIGATIONS

- Users can request a copy of everything they have shared on Instagram
- Users can view "Access Data" (Security settings)
- They **do not** require email or phone verification of the user
- They **do not** require users to use real names or identities



INSTAGRAM & LAW ENFORCEMENT

- “We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act (“SCA”), 18 U.S.C. Sections 2701-2712.”
- Need the username for the date range you are seeking information.

Instagram.com

FACEBOOK FEATURES



Create a
user profile



Have
“friends”



Can post
photos,
thoughts,
status
updates



Share
articles



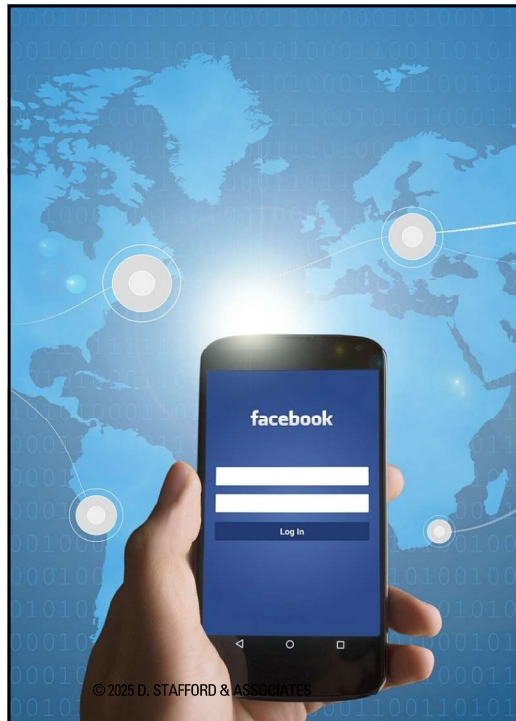
React to
posts



Can like
pages and
groups

ABOUT FACEBOOK

- Facebook's popularity is declining with teens and young adults though some still have accounts despite a lack of use
- Introduced the "like" button in 2009
- In 2020, Facebook launched "Campus" to address their declining numbers of college students; it was shut down in 2022
- Informal groups like "Buy or Sell" or "Barstool Sports" often spew dislike and anger



© 2025 D. STAFFORD & ASSOCIATES

83

FACEBOOK & INVESTIGATIONS

- Users can download their data through Privacy and Settings
- Try variations of names
- Utilize filters
- Search for known "friends"



© 2025 D. STAFFORD & ASSOCIATES

84



FACEBOOK & LAW ENFORCEMENT

- Facebook has received pressure to “crack down” on law enforcement for creating fake profiles.
- “We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act (“SCA”), 18 U.S.C. Sections 2701-2712.”
- Additional information is available on Facebook’s website.

Facebook.com

TINDER AND GRINDR FEATURES



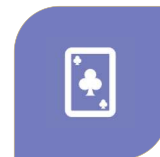
Create profile



Both utilize location-based matching



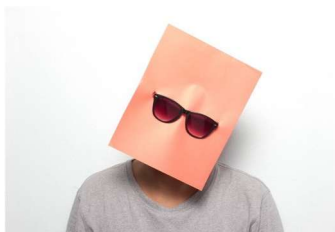
Grindr utilizes tile views and “taps” to indicate interest



Tinder uses card stack view and swipes right if interested, left if not

ABOUT TINDER AND GRINDR

- May be considered more “hook-up” apps than dating apps
- Tinder U: a version exclusive to college students
 - Must use .edu address
 - Other students from the same institution are shown first
- Grindr: Exclusively built for LGBTQ community
 - Most popular dating app for LGBTQ college students
- Easy to create “impersonation” profiles



DATING APPS & INVESTIGATIONS

- It is easy to impersonate someone else.
- Individuals may be embarrassed to share photos and messages.
- Investigators need to be comfortable discussing these apps and refrain from judgment.
- If the party has a parent/family member as an advisor, that may add a difficult dynamic.

TINDER & LAW ENFORCEMENT

- Tinder retains a user's data three months after an account is deleted or after two years of inactivity.
- Active users can download their data.
- No user verification.
- Response to Reports of Assault:
 - Tinder users can easily report instances of abuse or assault in-app or online. We strongly encourage any user who believes they have been a victim of a crime to report it to law enforcement. Our team works to promptly investigate reported crimes, assess and take appropriate action, and fully cooperates with law enforcement in any investigation.
 - When a user reports an assault to Tinder, we attempt to identify the alleged perpetrator and block the associated account. The incident is then reported to Match Group's centralized safety repository and checked across our various brands to see if the user has other accounts on other platforms. If any are found, they are blocked as well." (Tinder policies)



GRINDR & LAW ENFORCEMENT

- Once a message has been delivered to a recipient, Grindr deletes the data within 24 hours.
- Profile and location information of a deactivated user is deleted within seven days unless retained for a legal purpose.
- Chat images, user activity, and other Personal Data are deleted within 120 days of account deletion.
- Public information regarding interactions with law enforcement is limited to a request via an email address.

REDUCING YOUR DIGITAL FOOTPRINT

It's important to reduce your active and passive digital footprints — particularly if you're not trying to brand yourself professionally or scale a data-driven business.”

Here are a few ways to appropriately reduce your digital footprint:

- Close old or unused email accounts;
- Browse the internet in incognito mode to avoid cookies;
- Unsubscribe from unwanted email newsletters;
- Limit the information you share on social media;
- Keep your personal email address private;
- Regularly update your browser and privacy settings;
- Use virtual private networks (VPN) to stop web browsers from accessing your IP address and other data;
- Set [age-based internet safety restrictions](#) for children;
- Regularly update passwords used online.



<https://www.verizon.com/about/blog/digital-footprint-definition-examples-and-ways-reduce>

AIRTAGS & AIRDROP



Track airtag moving with you: <https://www.youtube.com/watch?v=mGh7-IuPRR4>
<https://youtu.be/y9QX-0IVQL4?si=a1R8BSNYpcd9Eo1m>

Privacy & Security



Information stored by websites on your devices, and these files can only be removed manually by you. This helps the website run faster and prevents information from being lost if you lose your connection. It is also used in a variety of other ways, such as personalizing your experience. There are session and persistent cookies. Information can include but is not limited to:

- **User Behavior**
 - Search history
 - Websites pages visited
 - Shopping cart items
- **User Identifiers**
 - Personally Identified Information (PII) “Online Forms”
 - Login details
 - Language Preferences

Federal Trade Commission (FTC) Cookie Uses

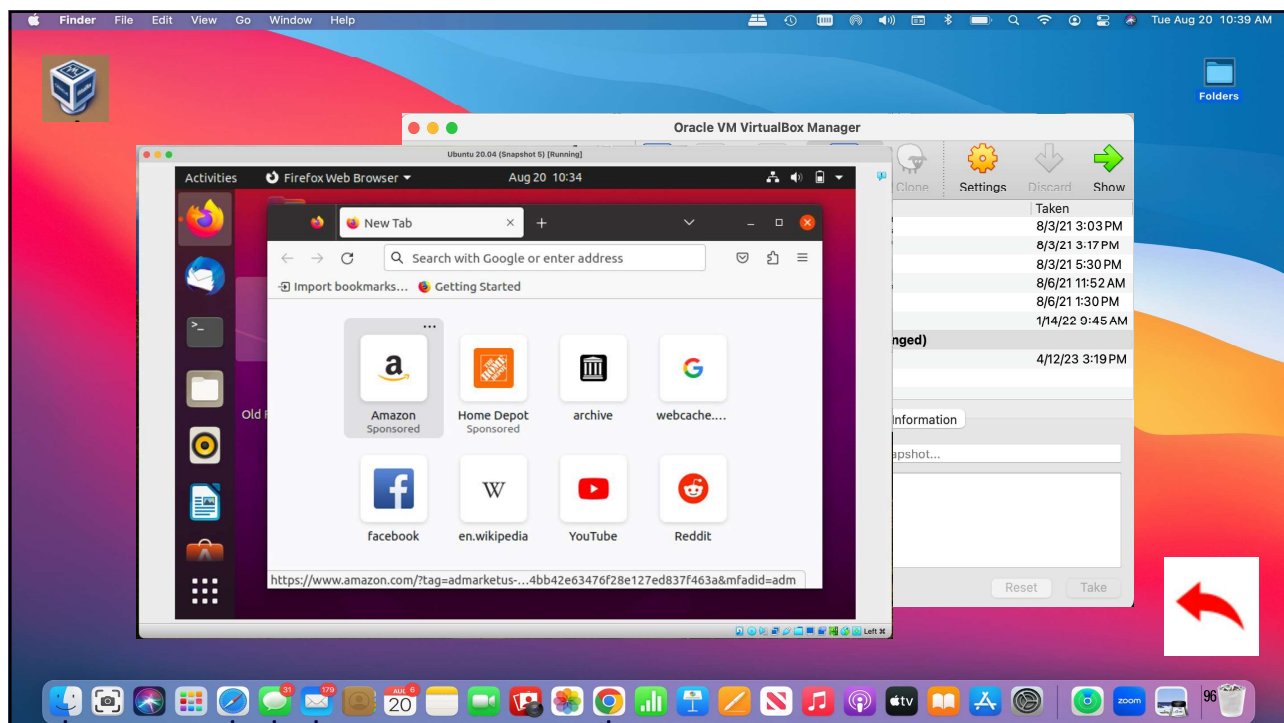
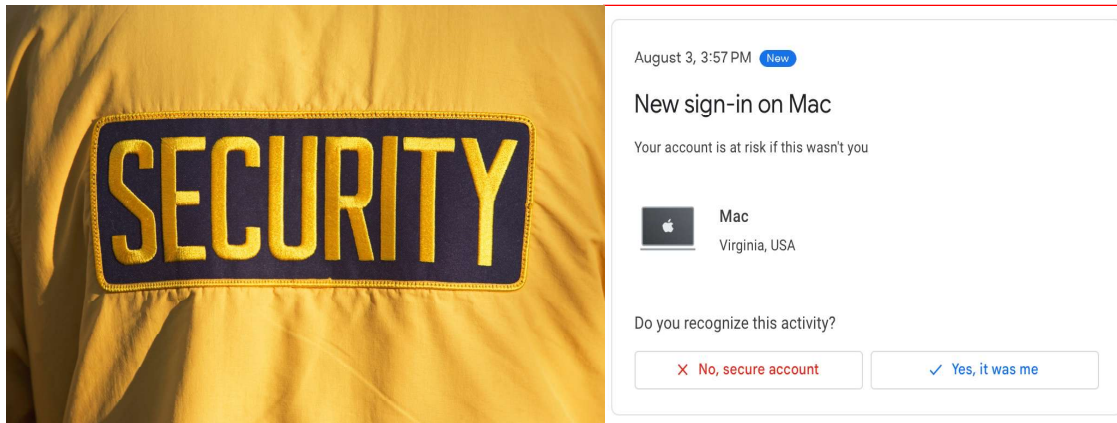
- <https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information>
- <https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies>
- Cookie Consent Banner – Improvement?
- <https://s3d.cmu.edu/news/2024/0505-cookies.html>

COOKIES



END-TO-END ENCRYPTION (E2EE)

- The sender’s message is turned into a code, and when the intended receiver gets it, it is decoded.
- Theoretically, only the users can read the messages.
- Challenges:
 - Man in the Middle Attacks (MITM)
 - Endpoint security
 - Backdoors
 - Compliance and regulatory requirements for content inspection





© 2025 D. STAFFORD & ASSOCIATES

MINI CASE STUDY #2 - BUCKLER CASE

To demonstrate digital evidence within Social Media, I sought a real investigation within publicly available court records. As Snapchat is a popular site, I sought a case where digital evidence was obtained through consent from a Snapchat account. I located following criminal complaint on Justice.gov, which I used to develop these case slides. Case is related to the events, which took place in and around the United States Capitol Grounds on January 6, 2021. I am solely using this case to demonstrate information that can be gleamed from Snapchat in support of an investigation and information you can gleam from publicly available court documents on reputable sites.

<https://www.justice.gov/usao-dc/case-multi-defendant/file/1434576/dl>

97



© 2025 D. STAFFORD & ASSOCIATES

MINI CASE STUDY #2 - BUCKLER CASE

United States of America v. Matthew Joseph Buckler

Tipster 1 (anonymous) stated BUCKLER had been inside the U.S. Capitol Building. He also provided a screen capture of allegedly BUCKLER's private Snapchat story and user's profile.

- Snapchat story and video showed:
 - An individual wearing a black jacket over a white hooded sweatshirt, and a black baseball cap.
 - User name "**matt's priv**" in upper right corner of video
 - User display name "**Matt Buckler**" displays at conclusion of video
- Snapchat user's profile showed
 - heatmap displaying a "bitmoji" labeled "Matt" placed prominently on top of a satellite image of the U.S. Capitol Building and grounds (Specifically, southwest corner of the U.S. Capitol Building)

Note: As noted in complaint, based on affiant's experience and training, "bitmojis" are stylized caricature which Snapchat users create as their online avatar and design, often, but not always, to mimic their actual physical appearance. Further, social media phone applications often use and capture location data based on cellular signal and a phone's Global Positioning System. The heatmap filter on Snapchat to display the user's location based on that locational data.

98



© 2025 D. STAFFORD & ASSOCIATES

MINI CASE STUDY #2 - BUCKLER CASE

United States of America v. Matthew Joseph Buckler

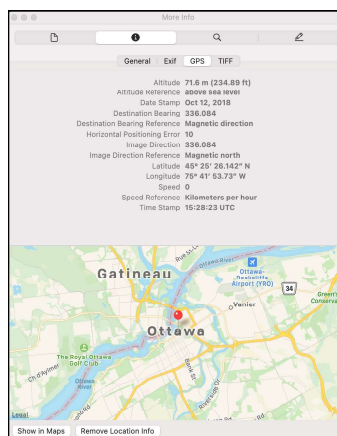
Tipster 2 provided Snapchat account mbuckler5 and advised it belonged to BUCKLER.

- Public search **mbuckler5** on Snapchat showed:
 - “matt” and bitmoji shows on profile
 - Bitmoji matches bitmoji in Snapchat screenshot provided by Tipster 1.
- Interview of Tipster 2 revealed:
 - Tipster 2 observed Snapchat posts from a known individual (Individual 1) which depicted both Individual 1 and BUCKLER on January 6, 2021, and present at the rally outside the U.S. Capitol Building, and inside
 - Tipster 2 also provided Individual 1’s cellular telephone number, leading to interview of Individual 1.
- Individual 1 was interviewed and acknowledged that the individual is well acquainted with BUCKLER, and that BUCKLER was inside the U.S. Capitol on January 6, 2021.
- Legal process was used to determine phone number associated with Snapchat account, mbuckler5 and subscriber information for the phone number linking BUCKLER to the SnapChat account. Phone records showed number utilizing a cell site for service in geographic area including the interior of the United States Capitol Building.

99



METADATA/EXIF



© 2025 D. STAFFORD & ASSOCIATES

100




EMAIL HEADER EXERCISE

Assignment:

A friend receives an email from Microsoft-noreply@Microsoft.com regarding a Microsoft order for Microsoft 365. He asks if you think it is legit.

- What would be your first question?
- What might you ask him to send you?
- What actions would you take to determine if this email was fraudulent?

From: Microsoft <microsoft-noreply@microsoft.com>
Date: Mon, 09 Dec 2024 at 6:09 PM
Subject: Your Microsoft order on December 9, 2024
To: <notification@merchantsales.onmicrosoft.com>

 Microsoft

Review details of your Microsoft order

Thanks for your order on August 16, 2024.

You can manage your subscriptions in the Microsoft 365 admin center.

[Go to Microsoft 365 admin center >](#)

Billing information		Order Id	
Support Helpline : 1-(805) 316-0078		ef1e8ee8-0480-494d-d07a-a75dfc39ca47	
Billing profile: 1 Microsoft Way Redmond, wa, 98052-8300			

Cloud	Your order items	Quantity	Unit price	Price
Global	Microsoft 365 Business Premium	1	\$792.00 USD	\$873.58 USD

Subtotal **\$873.58 USD**

Subtotal does not include any applicable taxes or fees except where specifically displayed on the invoice.
Please see your invoice for the final amount.



You request he forward you the email header and this is what you receive. What digital footprints can you find that might help to identify where email originates and if it is fraudulent?

EMAIL HEADER:

X-Spam-Flag: NO
Received-SPF: pass (mail163c40.carrierzone.com: domain of bounces+SRS=yz4se=TC@salescall948.onmicrosoft.com designates 104.47.55.174 as permitted sender) receiver=mail163c40.carrierzone.com; client-ip=104.47.55.174; helo=NAM12-BN8-obe.outbound.protection.outlook.com; envelope-from=bounces+SRS=yz4se=TC@salescall948.onmicrosoft.com; x-software=spfmltiter 2.001 http://www.acme.com/software/spfmltiter/ with libspf2-1.2.10;
DMARC-Filter: OpenDMARC Filter v1.4.2 mail163c40.carrierzone.com 4B9lhYi71461610
Authentication-Results: mail163c40.carrierzone.com; dmarc=pass (p=reject dis=none) header.from=microsoft.com
Authentication-Results: mail163c40.carrierzone.com; spf=pass smtp.mailfrom=salescall948.onmicrosoft.com
X-Envelope-From: bounces+SRS=yz4se=TC@salescall948.onmicrosoft.com
Authentication-Results: mail163c40.carrierzone.com; dkim=pass (1024-bit key, unprotected) header.d=microsoft.com header.i=@microsoft.com header.a=rsa-sha256 header.s=selector2 header.b=As91DDSJ; dkim=pass (1024-bit key, unprotected) header.d=microsoft.com header.i=microsoft-noreply@microsoft.com header.a=rsa-sha256 header.s=s1024-meo header.b=kJY4xT6+
Return-Path: <bounces+SRS=yz4se=TC@salescall948.onmicrosoft.com>
Received: from NAM12-BN8-obe.outbound.protection.outlook.com (mail-bn8nam12lp2174.outbound.protection.outlook.com [104.47.55.174]) by mail163c40.carrierzone.com (8.14.9/8.13.1) with ESMTP id 4B9lhYi71461610 for <victim@mail.net>; Mon, 9 Dec 2024 13:43:38 -0500
Resent-Date: Mon, 9 Dec 2024 13:43:38 -0500
Resent-Message-Id: <202412091843.4B9lhYi71461610@mail163c40.carrierzone.com>
Received: from DS7PR06MB6933.namprd06.prod.outlook.com (2603:10b6:5:2c4::7) by SJ2PR06MB9380.namprd06.prod.outlook.com (2603:10b6:a03:556::21) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8230.12; Mon, 9 Dec 2024 18:43:02 +0000
Received: from DS7PR06MB6933.namprd06.prod.outlook.com ([fe80::b2f9:3edf:9842:46cc]) by DS7PR06MB6933.namprd06.prod.outlook.com ([fe80::b2f9:3edf:9842:46cc%5]) with mapi id 15.20.8230.016; Mon, 9 Dec 2024 18:43:02 +0000
ARC-Seal: i=4; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=pass; b=slXN/ivdzo/q1kZZxKE6R5CNVxttJQU79ue9SyQa2peTNqo5OQ0VMYXejSvZmRzD6cKIN29u9EBIMFgy5nSg7q4lIjjh7DNuUhFQ6hkw+b7I5cYN0gM5pVdn7FmPFP4wbbSjmLED00XNKoeN6CrYy5rqqqnN8W4uh/q7vtKN1Dh5BVIYsYdTS7/+HG54OK/Wt0crullh9bS28v2kOnexOtc0BRHOb5yD3AdyjExMiY5BciitK0Bi3ufe3zpg1gJi/pLv2agxjXwZ2gklI8vQaU8m1HuU4I8I020x0ROUSpTVm8JzHMqRZi0CNXohsH0JBoqoEiDQbz77/zlnCtPpg==
ARC-Message-Signature: i=4; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-Mess
ageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-Messa
geData-1;
bh=7ROZvGHi4Si6bhVR9goBINscRrnLOXxu+RMvTV4SVYo=; b=x5vjSMUEWpWoWVuYpWwBjqz78/CerxIXEIP2yJzX3oeCuo7q2t60cnxtePekyY4ScKYbR98uOsYtS5EBq9
5ZkrQy+s4AdwPP6gSiVCcgHN+iCptPKhZiQs8C18N+XKv7aty6pwCkuLLGWkmwigRwTfK9QNJ5VjvTNCufmb
vF9GM4Rqk9umHQ1ruqhXj04o+aNP2sB74UsD7ZRzC54fTg0OEWEsUTelFTE+4+j7/hv7kDypfB/G6LnKf+Fe



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

MA2DlpH+JfCESFyP6XWz6Jz2Nm8rcJaUkFrPQRImJliY9aa2w+CH1oLhKgh+uiZ+rv43c+cBKT90daSzIHNZ
QwnOrzpg==
ARC-Authentication-Results: i=4; mx.microsoft.com 1; spf=pass (sender ip is
52.100.155.237) smtp.rcpttodomain=salescall948.onmicrosoft.com
smtp.mailfrom=0365bills.onmicrosoft.com; dmarc=pass (p=reject sp=reject
pct=100) action=none header.from=microsoft.com; dkim=pass (signature was
verified) header.d=microsoft.com; dkim=pass (signature was verified)
header.d=microsoft.com; arc=pass (0 oda=1 ltdi=1
spf=[1,3,smtp.mailfrom=microsoft.com] dkim=[1,3,header.d=microsoft.com]
dmarc=[1,3,header.from=microsoft.com])
Received: from BY3PR04CA0014.namprd04.prod.outlook.com (2603:10b6:a03:217::19)
by PH0PR06MB7095.namprd06.prod.outlook.com (2603:10b6:510:49::11) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8230.18; Mon, 9 Dec
2024 18:10:10 +0000
Received: from SJ1PEPF00001CE6.namprd03.prod.outlook.com
(2603:10b6:a03:217:cafe::8) by BY3PR04CA0014.outlook.office365.com
(2603:10b6:a03:217::19) with Microsoft SMTP Server (version=TLS1_3,
cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.12 via Frontend Transport; Mon,
9 Dec 2024 18:10:10 +0000
Authentication-Results: spf=pass (sender IP is 52.100.155.237)
smtp.mailfrom=0365bills.onmicrosoft.com; dkim=pass (signature was verified)
header.d=microsoft.com;dmarc=pass action=none header.from=microsoft.com;
Received-SPF: Pass (protection.outlook.com: domain of
0365bills.onmicrosoft.com designates 52.100.155.237 as permitted sender)
receiver=protection.outlook.com; client-ip=52.100.155.237;
helo=NAM10-BN7-obe.outbound.protection.outlook.com; pr=C
Received: from NAM10-BN7-obe.outbound.protection.outlook.com (52.100.155.237)
by SJ1PEPF00001CE6.mail.protection.outlook.com (10.167.242.22) with Microsoft
SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.7
via Frontend Transport; Mon, 9 Dec 2024 18:10:05 +0000
ARC-Seal: i=3; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=pass;
b=KEEXDbJ92nTFx76oEM1bsvTabaYEEq7ygcpx3WWiFa9kDFuJ0azmlajjhrB8BrGgQA6501CRnFLp5EWtF
JVkE/LooeS9yis/RNq1aQLASKckIUWf7t60UAEx+N+HvDOeuGiBYGCQM8sEEvwMRsdEkfK8s0mvvTlhQ0gf
vs8lyRQwV2jHZmd2AKpcMLa/IWg51qoohQWXJTuPq06qwFhdsMLPyWx/lki+3FYyveiWMpw3s4tkgzgEMh+Q
wVqzQ9mNLJOlcoKsJaOm027pHF3GtIT2CNXhoTXUCdTkTee5KDGh+oMuxo6tNKsvwxnWu63T8kvDCCg0CqBbf
NauqhFuA==
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
s=arcselector10001;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-Mess
ageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-Messa
geData-1;
bh=7ROZvGHi4SI6bhVR9goBINscCrnLOXxu+RMvTV4SVYo=;b=WkpWY2Jbz7enUHfAg4rk5VMQ+Wq4gvS6D+8asvfOTj6GT+OOqeCurgL1haammell
wQla0puWssUpiGJuCl
juVo4Fhy8RYv2DvVuc3n9uBA7DJWRzn1Kwmk0k8Z3VAeL0Iz7VgHYTEbBtd7yIN+0oLQuKIN6oWecjgXoFEq
e20v8FPPJUP4Re+Xbv2Fha8ubF9oF1Hcg8wl0MpSgk3J2R4ChvgJDykwXLfxrtajFEwBdGxD1voyjzqsAm4a
yNTzoRqDUk37t3HqW/xnXG+r6dWI8j5M7ysabwA9h6OHdwGLMztc+gD5WhGTsrzFv1GVgQV6MSj0faly5bhR
CBSiYYUg==
ARC-Authentication-Results: i=3; mx.microsoft.com 1; spf=pass (sender ip is
52.102.139.2) smtp.rcpttodomain=0365bills.onmicrosoft.com
smtp.mailfrom=microsoft.com; dmarc=pass (p=reject sp=reject pct=100)
action=none header.from=microsoft.com; dkim=pass (signature was verified)
header.d=microsoft.com; dkim=pass (signature was verified)
header.d=microsoft.com; arc=pass (0 oda=1 ltdi=1
spf=[1,1,smtp.mailfrom=microsoft.com] dkim=[1,1,header.d=microsoft.com]
dmarc=[1,1,header.from=microsoft.com])
Resent-From: <microsoft-reply@0365bills.onmicrosoft.com>
ARC-Seal: i=2; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=pass;



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

b=ny7TYIZGmVpSXji8SOe6W0cde8M4dHbjkeVc/Z8DXngLAAUuAXnseFuV2k6DW1YMTQNmnn+ApNHAmv3+ZbS
K7J5t6J9wSbw2UevrhaFABFNH8fGA5Qw5DIZVknjAJLtBIlf5AezkMbhZTnzhSxpUe83d0Lo1kGI5hqDdYLu
ViFal2qg6A9A45iGDUDv3vSfJYoTbL9pGeNtrn8zdGuk1e2QG6QOzOVHsUKaoBQEgc2YPYtXSSorLqf5LjQ4
Jbt7x2saMYbIAH9CfeyQ2S8tAMdETWjxVPHVatauDeBKMxbXrKXWt8MtyF8o+mPEpUxSd0yK3c3L3geFFeS
pEYBgnpQ==

ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
s=arcselector10001;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-Mess
ageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-Messa
geData-1;

bh=7ROZvGHi4SI6bhVR9goBINscCrnLOXxu+RMvTV4SVYo=;

b=B72S028Z4ooeoxCIZNOzzm4SoPHB3j/u2VPTUDTcJxCF58XC/mya/178qMdDHs2SyX9HVO7fo2gmdDrdlp
ewXkTKb88cmPEAfG5ZzqJoAAGr+xdBc4wl4k6rXV01VDfHWfWXdfZSaxXhisGqdUJG4aqXvGocT0zJ6jEuAY
q/WLAR2y86G9lCzMqra5Gk2QIDNYpjFbaK/Kf4PGV7ys0pEKgboyQnCzNGKdNIFcdpa5G9YMOKTcZCU0Imq1
p5ypO8tq17k2utiQEdigw+JoU23f5H5en32516K/hi/WVQevRrgPdtG5Jfn79ZlrBXlu+/AhMB5huMWepNji
9ql31h+g==

ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is
52.102.139.2) smtp.rcpttodomain=0365bills.onmicrosoft.com

smtp.mailfrom=microsoft.com; dmarc=pass (p=reject sp=reject pct=100)

action=none header.from=microsoft.com; dkim=pass (signature was verified)

header.d=microsoft.com; dkim=pass (signature was verified)

header.d=microsoft.com; arc=pass (0 oda=1 ldi=1

spf=[1,1,smtp.mailfrom=microsoft.com] dkim=[1,1,header.d=microsoft.com]

dmarc=[1,1,header.from=microsoft.com])

Received: from PH8PR22CA0023.namprd22.prod.outlook.com (2603:10b6:510:2d1::21)

by PH7PR18MB5550.namprd18.prod.outlook.com (2603:10b6:510:2f8::20) with

Microsoft SMTP Server (version=TLS1_2,

cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8230.18; Mon, 9 Dec

2024 18:09:55 +0000

Received: from SN1PEPF000397B2.namprd05.prod.outlook.com

(2603:10b6:510:2d1::cafe::d8) by PH8PR22CA0023.outlook.office365.com

(2603:10b6:510:2d1::21) with Microsoft SMTP Server (version=TLS1_3,cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.13 via Frontend

Transport; Mon,

9 Dec 2024 18:09:55 +0000

Authentication-Results-Original: spf=pass (sender IP is 52.102.139.2)

smtp.mailfrom=microsoft.com; dkim=pass (signature was verified)

header.d=microsoft.com;dmarc=pass action=none header.from=microsoft.com;

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

52.102.139.2 as permitted sender) receiver=protection.outlook.com;

client-ip=52.102.139.2; helo=DM1PR04CU001.outbound.protection.outlook.com;

pr=C

Received: from DM1PR04CU001.outbound.protection.outlook.com (52.102.139.2) by

SN1PEPF000397B2.mail.protection.outlook.com (10.167.248.56) with Microsoft

SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.7

via Frontend Transport; Mon, 9 Dec 2024 18:09:55 +0000

ARC-Seal: i=1; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=none;

b=c/xCx72yGWBw3ArjJ9De529s9Am9TH/wEnTU9khLs3GWS0dtOEQTCPEAtlmmG8hNk5HXZs5HGw72cSoJPY

rGR65rGZQFCNk+O2nF2TqHNWwXbAf3stJuP1E7ewQt52Awlsn4CHQqPg8rPsmoApKHzi1CYcy+fP+o+/unB

iwnKt01WvaIV4l+Beu6dia6vjvQ536/qAXPLL8l993ml8B0igMYs6l/mbbieMCu+XJosUvO3jJ4NqK7SYJHv

V9rP36LKq8eQn8f3Z4DBqnZJB4VpgpvBBdy0cA2T+ZqL5uaOR2ud3gpFOEUOYP2N2LXJcdJXnNRDRSW+TW

QBzfb1ng==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;

s=arcselector10001;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-Mess

ageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-Messa

geData-1;

bh=7ROZvGHi4SI6bhVR9goBINscCrnLOXxu+RMvTV4SVYo=;

b=VXg20va6W7uV3iU6l88Y0OPIKrnkqgR1e0Lk1BVRcdLE8P+ScZyy7ZlxY0FDjXxThD3qTCqupJKRUdya1J



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

k9XZTRrZuroqEU85ODk8SZA0Isl0o9g3nzWVWTcVWUaZXAKQHunROpy3onMEpV5O0yzB3n+TXQZQWfPgF+B
UlW0ZkU0SUYS8l0uqP3bVvAdXNMuawtQcfSC9ulUMRr8lmNyXzQQSph6vdmN8mn8sl4cv1byFJ/dbR9EHn/W
2XexlrLShWx4el9e9eLCJxBwRsNkl6GMicyhin25G3Lr/JM0YthAuY17a1k1mcHP7GceMmBNS0MPR/W16lly
DCGVYUZg==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass (sender ip is
20.97.34.221) smtp.rcpttodomain=0365bills.onmicrosoft.com
smtp.mailfrom=microsoft.com; dmarc=pass (p=reject sp=reject pct=100)
action=none header.from=microsoft.com; dkim=pass (signature was verified)
header.d=microsoft.com; arc=none (0)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
s=selector2;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck
;
bh=7ROZvGHi4SI6bhVR9goBINscCrnLOXxu+RMvTV4SVYo=;
b=As91DDSJP1wvTOrHIVZWDxvgcfKVVW3d/bMY0bD3AWmHtHtbfileS+7BL0juC6h4WO6KttedLDGCWylCrG5
ef07X1UYM88GvgD6e7RjJctLvOtrniF0tFwLDyqjGVmictU+Zaq6yJlt3pGi+RGjhKNsWIPFmgj6NCCeumH
EEvx4=
Received: from BN0PR03CA0038.namprd03.prod.outlook.com (2603:10b6:408:e7::13)
by DS1PR21MB4379.namprd21.prod.outlook.com (2603:10b6:8:207::8) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8251.12; Mon, 9 Dec
2024 18:09:50 +0000
Received: from BN1PEPF00005FFC.namprd05.prod.outlook.com
(2603:10b6:408:e7:cafe::36) by BN0PR03CA0038.outlook.office365.com
(2603:10b6:408:e7::13) with Microsoft SMTP Server (version=TLS1_3,
cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.13 via Frontend Transport; Mon,
9 Dec 2024 18:09:49 +0000
X-MS-Exchange-Authentication-Results: spf=pass (sender IP is 20.97.34.221)
smtp.mailfrom=microsoft.com; dkim=pass (signature was verified)
header.d=microsoft.com; dmarc=pass action=none header.from=microsoft.com;
Received-SPF: Pass (protection.outlook.com: domain of microsoft.com designates
20.97.34.221 as permitted sender) receiver=protection.outlook.com;
client-ip=20.97.34.221;
helo=mail-nam-cu04-sn.southcentralus.cloudapp.azure.com; pr=C
Received: from mail-nam-cu04-sn.southcentralus.cloudapp.azure.com
(20.97.34.221) by BN1PEPF00005FFC.mail.protection.outlook.com
(10.167.243.228) with Microsoft SMTP Server (version=TLS1_3,
cipher=TLS_AES_256_GCM_SHA384) id 15.20.8230.7 via Frontend Transport; Mon, 9
Dec 2024 18:09:49 +0000
DKIM-Signature: v=1; a=rsa-sha256; d=microsoft.com; s=s1024-meo;
c=relaxed/relaxed; i=microsoft-noreply@microsoft.com; t=1733767789;
h=from:subject:date:message-id:to:mime-version:content-type;
bh=7ROZvGHi4SI6bhVR9goBINscCrnLOXxu+RMvTV4SVYo=;
b=kJY4xT6+E15R8ZKTrxz0YS71dSAFJt+aqI/ZK+ovpgh2UiDyHLfSb9RNYcCq03T/salX98dKqmt
JET8Q+vnUCn6PuhTBrFO00/6k2B5I8UI5Rw/d0xlseKZ1zi0Mx9qjAtQ2d3sKztglOFmV52mevhcd
Cdf8ZoUG8Otp9I6trcs=
From: Microsoft <microsoft-noreply@microsoft.com>
Date: Mon, 09 Dec 2024 18:09:49 +0000
Subject: Your Microsoft order on December 9, 2024
Message-ID: <2a354646-42a6-44f5-bb3c-3c99d842330f@az.southcentralus.microsoft.com>
To: microsoft-reply@0365bills.onmicrosoft.com
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="=-uWTn7xaX7Ax2N833CUB61Q=="
X-EOPAttributedMessage: 2
X-MS-TrafficTypeDiagnostic:
BN1PEPF00005FFC:EE_IDS1PR21MB4379:EE_ISN1PEPF000397B2:EE_IPH7PR18MB5550:EE_ISJ1PEPF0
0001CE6:EE_IPH0PR06MB7095:EE_ISJ2PR06MB9380:EE_
X-MS-Office365-Filtering-Correlation-Id: 8ad41580-681b-4795-263d-08dd187cb806
X-MS-Exchange-SenderADCheck: 1



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

X-MS-Exchange-AntiSpam-Relay: 0
X-Microsoft-Antispam-Untrusted:
BCL:0;ARA:13230040I240411011799012I1800799024I36860700013I11053499020;
X-Microsoft-Antispam-Message-Info-Original:
=?us-ascii?Q?NymK41bxeTPuzVHVUEXZNRhf9DDfKtZ18iaHrh+0hp+HQO9H0mK3zUWB6/iv?=
=?us-ascii?Q?STVTxOI5c8V8Bau+eTi9Es9TyZy46fv6BNnE3EdKqPAFiCLbgADgt86t4CS?=
=?us-ascii?Q?p6X3RjmwvG4fyQJvr6Mp69K2s5iLimNiWe/tHDeq64jUc05Ao57Z9EdfDBD+?==?us-
ascii?Q?KIT7swgr+tdS2IiUtuCXQB7AGBjrSPLBy6ygoacsxmQ3tC4HHPk8v9Rhgpts?=
=?us-ascii?Q?51SxpSFGI+TeDJK+Zq0ltEEqJ6GcRAawbnB3GmVZqt668UI42nsEbt6sBq3e?=
=?us-ascii?Q?BML+Thh8hz60RFGIfLmEQeDnLTpdgprTZr2Hd0Bmxl9vcKLncCyqUql+4tOy?=
=?us-ascii?Q?3kmrVfk4JGkFQHzmvMvi4Ko1IEjgnOXBk8FchJnJiN06jVITssQZC1ZjQk5j?=
=?us-ascii?Q?OpUL9d+oLw6Oy2GmHnjSJ9//s0w0NC2aPwl9pqlpr+XzN4o450jsHoTabD1?=
=?us-ascii?Q?aEhLNRrZj+0mJ2npFy9qqobBeqZwS5hhJ/veB4E/m0DSfmrkvb45gERrKN6i?=
=?us-ascii?Q?DAQ/1FsuESnLDIOk/fPOCoyUeAJ1R2Z92JfNase/tQ+SLaLa82Oo1sxhGXxd?=
=?us-ascii?Q?S3TIOiYnROaZRtbrZGytqIGHkaG77Ho+F8yesEOaE7j/pUsFAZtYEGMacb3/?=
=?us-ascii?Q?KeC9MiDONajPdaltEtC9ulHG1JApl3HaR6YRRxosECIFL18p5M6nBKDp7GE?=
=?us-ascii?Q?reAJeCezlhFj946XZiaD33yvUq4FF4RcEf8ZJEHikUdAC8XJGPSRzmAeYFAS?=
=?us-ascii?Q?/h3XG+BLZ+u0J3p56XVnAH1s9HuYytJRdVLE/ng9AoVCt52uc3kUYtyA24CW?=
=?us-ascii?Q?xVzZz8Bx4LLFky6d3lpM+AVaC786QVH/VVw5y9Zn8uoCflvJOSkXXi3o/rNo?=
=?us-ascii?Q?ceeRw+YQzPZOFR485R0N3brVMzjMgPI53826ONHztGaXwZaWc1lkDDdDbBBZ?=
=?us-ascii?Q?WbEjW4oq6WmK6ybEe8jPWF4NF1IOT4LMz0NL9/EaX0G4rRqHgVYVSL6h6yf?=
=?us-ascii?Q?NSlwTYWbkBSdWVU3Abv4CLo07r2xEdGPYfXYw+0ATnKLCDiQM31zUVlj37mL?=
=?us-ascii?Q?ielPI3PkyO7UqfnRf5Ay7kc6Zcu7tDR9pTiosSDtVa3F91IT7fRTY8vKC/qg?=
=?us-ascii?Q?bMFYDIW2ZrLNCYEsRssvQ5lateaeSvx8jrTAtPPkqnEe4DB+Pq5IILv9958?=
=?us-ascii?Q?SI2Fo74v8PPIF5RiCCtRT+qh1PreNfTcDJ+0oC2NVUatKxij894L0pke6ZT8?=
=?us-ascii?Q?Shdsl4XX6UfClxyLYh299/y7OxD7aAx7MZnCuG7ePMY5ylXUU/XzZ7udm2NF?=
=?us-ascii?Q?WyuLJG2d2TPk2kpnxCf2iJ4XW/u+NXbEJqWPLLXOKXIRfyup25B9YcfR7KTT?=
=?us-ascii?Q?4Cy6M95QPndF9v/TqD5PUcROh1LgiKr/CfN1N9DF0KbYuUr5fF6zSf9IxdQF?=
=?us-ascii?Q?1fU6KsrXsgChA2gvg/6IM+Cef+rTOE1naJ9e2u54uLnwtRdPCQg/CHof9oog?=
=?us-ascii?Q?BV49RR0BNTDu3asjw0dttv6sHtWs6xhDsaMDocnG3tp19jc88StSWgOPG3H9?=
=?us-ascii?Q?TycUNLnTZ/OcoYzVsGjtQkrAkqbawAqzetu0ruxDdAuxtziSMWUZkYmOSj9F?=
=?us-ascii?Q?taO6QgxvzjktT/3UmXSit0gKld+ldcdSIBQ6DvW39dUAgLrAsPjImEIDz3Pf?=
=?us-ascii?Q?VYWO7vc4p6aKYUj1Z/jmE3OliOeBAdiq6fkZY9zZINHNm4N5GK7sUtMdmT1G?=
=?us-ascii?Q?eE2AfCDuQSyEIRcgmBczleriuQ9Zes06rZmsNhT5EDQtqdGK+0Xo8Df7P8gB?=
=?us-ascii?Q?3eP+mwfhlglbMYOKsM/QEMJdJD0L8CJo/ppzRugb++9qWxrfnXkLZf3zk84u?=
=?us-ascii?Q?nshosqWjLi1kVxj5dK0cCxadK2ysz/bAS0f8Bh3rTkDJG0yXK9KzAz7GQ2S1?=
=?us-ascii?Q?OSO10dsd31y0TY03b1AcFYcYB4IRQSQ+ZTORx5qfRLHhNRG1Xdd+xeVcSzk?=
=?us-ascii?Q?nHdQR6tccUhXzRkjtCpofBftFovnX0DZNwDOCEgs4Gs4unEglOr6m5GRq5q?=
=?us-ascii?Q?4P9o73E30gpAj+mXVVOzFo13Mjy1gg=3D=3D?=
X-Forefront-Antispam-Report-Untrusted:
CIP:20.97.34.221;CTRY:US;LANG:en;SCL:7;SRV:;IPV:NLI;SFV:SPM;H:mail-nam-cu04-south
centralus.cloudapp.azure.com;PTR:mail-nam-cu04-southcentralus.cloudapp.azure.com;
CAT:OSPM;SFS:(13230040)(240411011799012)(1800799024)(36860700013)(11053499020);DIR:O
UT;SFP:1501;
X-MS-Exchange-Transport-CrossTenantHeadersStamped: DS1PR21MB4379
X-MS-Exchange-Transport-CrossTenantHeadersStripped:
SN1PEPF000397B2.namprd05.prod.outlook.com
X-MS-Exchange-Transport-CrossTenantHeadersPromoted:
SN1PEPF000397B2.namprd05.prod.outlook.com
X-MS-Office365-Filtering-Correlation-Id-Prvs: f4d805c4-d4be-432f-dd49-08dd187cac09
X-LD-Processed: 571ac94a-7f78-4238-bdc4-0835ba25833e,ExtAddr,ExtFwd
X-Microsoft-Antispam-Untrusted:
BCL:0;ARA:13230040I9140799003I14060799003I58601717416014I34036016I376014I69100299015
I35042699022I48200799018I11053499020;
X-Microsoft-Antispam-Message-Info-Original:
=?us-ascii?Q?owvHS6OKvpukjUtuu/AMM3qUGiyCniCBZjoJclS6MTu1kTRCxi2RkRiDaQ?=
=?us-ascii?Q?JzNliAlrOrZnL+Lut5OK2dzbuK3ODcaOgH/5vFOCrPDuhD9YI65M8pQOC9H?==?us-
ascii?Q?x3GuNMtzHZEslMalab8Pb/GuNwi8GhYbrLgxz2vvjJGxa3b6scEziLAVjpTh?=



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

=?us-ascii?Q?iRQtOvkXHKSnCLYbE3ovQeN2TGfOABhAxQ/39wgnRMDh3CG58Tec1ZHGxkmm?=
=?us-ascii?Q?ICib9/Z3HuGtr6vrY65u315OAqiTYAruEWtbD8sW45+Fcks0fTRivQuGWSmE?=
=?us-ascii?Q?vYnOCIPJgwwjvQxt+nCPeScJaRxWk97vTjjq+ml/CG+0fHB7dIYPK1xkXmVu?=
=?us-ascii?Q?IBMD6NvA3sOrRVFQv3gy9Q7NgkrWtSPy9PWHCYixWgANNoyXszNCBwY2bu1?=
=?us-ascii?Q?0CHqSP8Xb+bGQc6EckbVyPblEsNXfioptDYDabUsRFO5APdvZzp1uk/paN?=
=?us-ascii?Q?sX9Ez5up4wpmgd/z6RzjfaJr/Psk3xIBg+j07PSt3AxSC6ojlzd4kz3ibB9?=
=?us-ascii?Q?U2EQUcziXUIMBWc9EY0YuZyLjGQ8mq8D/mAazK+9UFhl/njloi3MhvMvKiB?=
=?us-ascii?Q?a7LCzLdGiPd58aJ9TsVtwhlyzIV9R9xRZa60kNkkol3YcnrdudOleLu+grRq?=
=?us-ascii?Q?B0snBtBH0TVPk9bODlyqeGe2OLZqKNkHX0l8Ne4P2AZXZKB+8t3DIVX6CUAf?=
=?us-ascii?Q?NNEvLbHPY+2izB4r2GhUndmZFEfzI0eMaiCZdPedVrgxepourrVvYg4j7mGv?=
=?us-ascii?Q?gvQILVq8BuOWGAad615jIXRdulqO0O3g7rv50EzvSDAMltzATWbeEo+oMFJP?=
=?us-ascii?Q?Gkcq8mHle2xK5g86e4S2FaQ8CfPBm8abyW0MiQ307/SB4zWMW2p84G9EoYEA?=
=?us-ascii?Q?d4ITvgMrzryl+L7eKAjx/F/NdqYKMMPoEtsQbwm0DlwNnxEgazP5Fg6o6uIH?=
=?us-ascii?Q?cV93SjYjRWUxBrudQS6kfsmes97x/QEKl9jP6xiLPDZ3Dyv1f3f3U3vKoGyG?=
=?us-ascii?Q?FbrwmnnvIQf0ll+6Nc7feF2AxM20dUYd5zzLQnmsdrtS5ZktlHhgQfM6e7G2?=
=?us-ascii?Q?XLf+YjJJK4POYF6lDHHGmqDYFJ7f/xY0mEcOfL0tFWYgOdOgntB6Swvp5cTb?=
=?us-ascii?Q?XquQzewe22K4vm36r9geNRZViuO/pk1ieZOvXuGAjIw2Z9pZUWuzJzWo9r0I?=
=?us-ascii?Q?Wdr/6Fvm240MwEALOGSIZpaT1TG3N4w+PDBd/kXivgSjdquqp0B77Z4HH612?=
=?us-ascii?Q?MPfyZK/tHt2B6TQBBw9X+F+9h+kpv4ERwM6vF56LDR0PuSPwzLOy6SbpmSAK?=
=?us-ascii?Q?10bi6cOI/dU7WJeM3c2slrTW8BB8s6lJz115L0gEMQWadgWH3R6xqkdGw+MI?=
=?us-ascii?Q?X0vB7xd9RBwBHgwZynMwYY8ooSVRclISFZf5PBjhwkNPXasFpwI3fRoryLVj?=
=?us-ascii?Q?bHdCjzg2jle6lkK5smxqjDX63sUhuaFUREOPpXTOMAnvT37QTt0PvKcDfBKE?=
=?us-ascii?Q?FOX5HvSrZ+4DK05CiRkebVZAnToLS5BLjmH/bADVul5y5Vx7cLf475JPI4m?=
=?us-ascii?Q?wnXCLrFH1ddpMGEk5gRTk20NxeJqQTOAEL1YV6pfny5w4TzZZdQgrTals2bV?=
=?us-ascii?Q?8fWmG/l8efyjqE4BywYAnod5O94yXZIPAMXJF6P66Enp8mEl0pqtN8H0gtxo?=
=?us-ascii?Q?p8b+iSxahYFLKdxlUhzC76RkGfXbcuznvNKArSy45Wv++a2XUvErRNAjJs18?=
=?us-ascii?Q?EqCGkNqUPnjlh9fhA+sSEKU46qbdV1SiKrk5idLHYhLZpLR350dS37FruUh/?=
=?us-ascii?Q?lhYYeyzNfdDkPrVfxr0RKHV2esSBtmc5O+A0f+8VWuuODPwxOp8eK+xnsYO?=
=?us-ascii?Q?QH2h72lSLThAjHo7d8oHlsR8tFyoJH5gx+GX2LBt4MsfAPGdChw7PA4CnWo?=
=?us-ascii?Q?Lb1pQUntOTuFWDAeqEcntqw=3D=3D?=
X-Forefront-Antispam-Report-Untrusted:

CIP:52.102.139.2;CTRY:US;LANG:en;SCL:7;SRV:;IPV:NLI;SFV:SPM;H:DM1PR04CU001.outbound.
protection.outlook.com;PTR:mail-centralusazhn15010002.outbound.protection.outlook.co
m;CAT:OSPM;SFS:(13230040)(9140799003)(14060799003)(586017)(7416014)(34036016)(376014
(69100299015)(35042699022)(48200799018)(11053499020);DIR:OUT;SFP:1501;
X-ExternalRecipientOutboundConnectors: 571ac94a-7f78-4238-bdc4-0835ba25833e

X-Auto-Response-Suppress: DR, OOF, AutoReply

X-MS-Exchange-Transport-CrossTenantHeadersStamped: PH7PR18MB5550

X-EOP-TenantAttributedMessage: a1f1959f-75bc-41ec-a13f-c3d7c4fb657c:0

X-MS-Exchange-Transport-CrossTenantHeadersStripped:

SJ1PEPF00001CE6.namprd03.prod.outlook.com

X-MS-Exchange-Transport-CrossTenantHeadersPromoted:

SJ1PEPF00001CE6.namprd03.prod.outlook.com

X-MS-PublicTrafficType: Email

X-MS-Office365-Filtering-Correlation-Id-Prvs:

7311ebc2-a983-40f6-77c5-08dd187caf5c

X-Moderation-Data: 12/9/2024 6:43:01 PM

X-LD-Processed: a1f1959f-75bc-41ec-a13f-c3d7c4fb657c,ExtAddr

X-OriginatorOrg: salescall948.onmicrosoft.comX-MS-Exchange-CrossTenant-Network-Message-Id: 8ad41580-681b-4795-263d-08dd187cb806

X-MS-Exchange-CrossTenant-Id: a1f1959f-75bc-41ec-a13f-c3d7c4fb657c

X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp:

TenantId=72f988bf-86f1-41af-91ab-2d7cd011db47;Ip=[20.97.34.221];Helo=[mail-nam-cu04-
sn.southcentralus.cloudapp.azure.com]

X-MS-Exchange-CrossTenant-AuthSource: SJ1PEPF00001CE6.namprd03.prod.outlook.com

X-MS-Exchange-CrossTenant-AuthAs: Anonymous

X-MS-Exchange-CrossTenant-FromEntityHeader: Internet

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 09 Dec 2024 18:43:02.6793

(UTC)



D. STAFFORD & ASSOCIATES

179 Rehoboth Avenue, #1121
Rehoboth Beach, DE 19971
searches@dstaffordandassociates.net

X-MS-Exchange-Transport-CrossTenantHeadersStamped: SJ2PR06MB9380
X-VADE-SPAMSTATE: spam:low
X-VADE-SPAMSCORE: 290
X-VADE-SPAMCAUSE:
gggruggvucftvghtrhhoucduddrgeefuddrjeeigdeklecuteufuodetggdotefrodftvfcufhrhohfihhl
vgemucfjqffvffqrrfktdpfgffpggdqveegtdeuceurgihlhouhhtmecufedtudenucdnvehorghstgr
lhculdefddtmdenjfgmrhvjvggrugvrhfhghvlgguucfjvggrugvrhcuufgtohhrihnhgculddquddt
mdenucfjughrpefhffkfvgggtsegrtderrdtdejnecuhfhrohhmpefoihgtrhoshhofhtuceomhhi
tghrohhsohhftdqnhhorhgvphhlhiesmhhiitghrohhsohhfthdrtghomheqneucggftrgrthtvghrnhp
udegveefhfkfhfiefvgeufeduffegjeduheekjefgleegfeegudfhveeieeunecuffhomhgrihnpegr
iihurhgvrdhnhvgthpdmihgtrhhoshhofhtrdgtohhmnecukfhppedutdegrdegjedrheehrddujeegpddv
tddrleejrdefgedrvddvdenucevlhushhtvghrufhiiigvpedtnecurfgrhgrmhpeihhnhvgthpedutdeg
rdegjedrheehrddujeegpdhvhghloheppfetofduvddquefpedqohgsvgdrohthuthgsohhunhgurdhprhho
thgvtgthihonhdrohthuthlohokhokdrtghomhdpmhgrihhlfhrohhmpegssohhunhgtvghsodfuffupeih
ieegshgvpefvveesshgrlhgvshgrghllhelgeekrdhonhmihtgrhhoshhofhtrdgtohhmpdhnsggprhgt
phththopedupdhrtghphthtohepvhinhgtvgesrhhiuggvshgsihhkvghsrhnhvght
X-Rspamd-Status: No, score=0.45
X-Rspamd-Result: default: False [0.45 / 6.00];
FORGED_RECIPIENTS(2.00)[m:microsoft-reply@0365bills.onmicrosoft.com,s:victim@mail.net
];
DWL_DNSWL_LOW(-1.00)[microsoft.com:dkim];
ARC_ALLOW(-1.00)[microsoft.com:s=arcselector10001:i=4];
URI_COUNT_ODD(1.00)[25];
DMARC_POLICY_ALLOW(-0.50)[microsoft.com,reject];
FORGED_SENDER(0.30)[microsoft-noreply@microsoft.com,bounces@salescall948.onmicrosoft
.com];
R_DKIM_ALLOW(-0.20)[microsoft.com:s=selector2,microsoft.com:s=s1024-meo];
R_SPF_ALLOW(-0.20)[+ip4:104.47.0.0/17];
MIME_GOOD(-0.10)[multipart/alternative,text/plain];
RCVD_NO_TLS_LAST(0.10)[];
MANY_INVISIBLE_PARTS(0.05)[1];
MIME_TRACE(0.00)[0:+,1:+,2:~];
RCPT_COUNT_ONE(0.00)[1];
MISSING_XM_UA(0.00)[];
ASN(0.00)[asn:8075, ipnet:104.40.0.0/13, country:US];
DKIM_TRACE(0.00)[microsoft.com:~];
NEURAL_HAM(-0.00)[-0.989];FROM_NEQ_ENVFROM(0.00)[microsoft-noreply@microsoft.com,bounces@salescall948.onmicro
soft.com];
FROM_HAS_DN(0.00)[];
RWL_MAILSPIKE_POSSIBLE(0.00)[104.47.55.174:from];
TO_DN_NONE(0.00)[];
URIBL_BLOCKED(0.00)[NAM12-BN8-obe.outbound.protection.outlook.com:helo];
TAGGED_FROM(0.00)[SRS=yz4se=TC];
MID_RHS_MATCH_FROMTLD(0.00)[];
RCVD_COUNT_SEVEN(0.00)[11]
X-Origin-Country: US
X-WHL: LR



Title IX Investigator Technology and Investigations (Tier 6)
Training Hyperlinks (08/21/2025)

- Digital Footprints
 - Setting Privacy Settings “Funny Example”: <https://www.youtube.com/watch?v=yriT8m0hcKU>
 - Reducing your digital footprint: <https://www.verizon.com/about/blog/digital-footprint-definition-examples-and-ways-reduce>
- AirTags & Airdrop
 - Track Airtag Moving with You: <https://www.youtube.com/watch?v=mGh7-luPRR4>
 - iPhone Safety check: <https://youtu.be/y9QX-0IVQL4?si=a1R8BSNYpcd9Eo1m>
- Electronic Communications Privacy Act (“ECPA”) & Stored Communications Act (“SCA”)
 - <https://www.iacpcybercenter.org/prosecutors/8-2relevant-federal-statutes/>
- Federal Trade Commission (FTC) Cookie Uses
 - <https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information>
 - <https://www.ftc.gov/policy-notice/privacy-policy/internet-cookies>
- Cookie Consent Banner – Improvement?
 - <https://s3d.cmu.edu/news/2024/0505-cookies.html>
- DNS tools
 - nslookup.io - Whois
 - centralops.net/co/ - Whois, Traceroute, etc.
 - whois.domaintools.com - Whois, Reverse Lookups, etc.
 - www.domain.com/whois/whois - Who owns & availability
 - www.bluehost.com/help/article/dns-records-explained - DNS explained
- How to find MAC Address on Device
 - <https://www.cmu.edu/computing/services/endpoint/network-access/mac-address.html>
- Firefox Browser – website information stored on your device, how much space is being used and how to free up space
 - https://support.mozilla.org/en-US/kb/storage?as=u&utm_source=inproduct&redirectslug=permission-store-data&redirectlocale=en-US



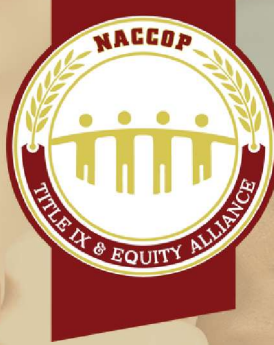
- Locate Vendor related to MAC address
 - Application: Wireshark: <https://www.wireshark.org/>
 - Online Tools: MAC Address Lookup: <https://macvendorlookup.com/>
- Provider Privacy Policies Examples & Obtaining Records
 - Directv: <https://www.directv.com/privacy/video-privacy-policy/>
 - Verizon: <https://www.verizon.com/privacy/your-data>
 - YouTube: <https://www.youtube.com/watch?v=3GV89k7c99g>
- Social Media/Dating Apps Policies Examples & Obtaining Records
 - YikYak: <https://yikyak.notion.site/Yik-Yak-Privacy-Policy-4cba37f3c1c94f0dae9fb2cc5cd8e3>
 - TikTok: <https://www.tiktok.com/feedback>
 - Snapchat: <https://support.snapchat.com>
 - Instagram: <https://help.instagram.com/>
 - Facebook:
 - <https://facebook.com/help/>
 - <https://www.facebook.com/privacy/policy> – record retention
 - Tinder: <https://www.help.tinder.com>
 - Grindr: <https://help.grindr.com>
- Time - Convert UTC to EST
 - <https://www.utctime.net/utc-to-est-converter>
- Google TakeOut Example
 - www.youtube.com/watch?v=yriT8m0hcKU
- ISPs from tracking your browsing history
 - <https://www.youtube.com/watch?v=3GV89k7c99g>
- Threat – Going across platforms (Droid to iPhone)
 - <https://www.cnn.com/2024/12/15/why-the-fbi-wants-you-to-use-end-to-end-encrypted-messaging.html>
- Extraction Tool (e.g. iMazing for Apple Devices, Droid Transfer or SMS Backup+)
 - iMazing Demo: <https://www.youtube.com/watch?v=FHZc04xCa0>



- Check if your email or phone has been in a data breach
 - <https://haveibeenpwned.com/>
- Spoof Messages
 - <https://www.youtube.com/watch?v=uJBZd2ZtgIc>
- Creating Fake Messages
 - App: ios8text.com
 - Demo: - <https://www.youtube.com/watch?v=E1qcOpUEXec>
 - Other references:
 - https://www.reddit.com/r/FakeTexts/comments/sxkgk3/ios_15_fake_text_generator/?rdt=39360
 - <https://ifaketextmessage.com>
 - <https://www.phonegags.com/>
 - <https://www.aicut.pro/tools/faketextmessagescreator>
 - <https://nastia.ai/tools/fake-text-message-generator>
 - <https://prank.chat/sms>
- Deepfake Scams
 - AI Roker's Image used in deepfake scam: <https://www.youtube.com/watch?v=x-M0wO0hn3E>
 - AI-Powered Deepfake Tools: https://www.trendmicro.com/en_us/research/24/g/ai-deepfake-cybercrime.html
- Online Communications:
 - Terms: <https://www.urbandictionary.com>
 - Sexual Emojis: <https://gabb.com/blog/sexual-emojis/>
- Web Archive
 - <https://web.archive.org/>
- Removing explicit or intimate personal images
 - <https://support.google.com/websearch/troubleshooter/3111061?hl=en>
 - <https://help.instagram.com/>
 - <https://cybercivilrights.org/ccri-safety-center/#online-removal>
 - <https://stopncii.org>



- Open Source Intelligence Tools:
 - OSINT Framework: <https://osintframework.com/>
 - IRB Search: <https://irbsearch.com/>
 - Court Documents & Records:
 - Pacer - <https://pcl.uscourts.gov/pcl/index.jsf>
 - Justice.gov - <https://www.justice.gov/>
(e.g., Searching Criminal Complaints)
 - Property Records Example:
 - Lynchburg, VA - <https://mapviewer.lynchburgva.gov/ParcelViewer/Account/Logon>
 - Vehicle Records:
 - NHTSA Recalls - <https://www.nhtsa.gov/recalls>
- University related cases:
 - Tyler Clementi Case: <https://youtu.be/EvjGTnG9Y40>
 - Lauren McCluskey Case – ABC News interview with parents: [youtube.com/watch?v=TlVsm_Fcia4](https://www.youtube.com/watch?v=TlVsm_Fcia4)
- D. Stafford Training Opportunities
 - <https://dstaffordandassociates.com/>



NACCOP Title IX & Equity Alliance

The Alliance is a dedicated affinity group through which Title IX and Equity Professionals, and the practitioners who support and/or supervise them, can benefit from NACCOP's expertise in complying with the Clery Act, Title IX, and other civil rights laws that affect their work.

BENEFITS OF JOINING THE ALLIANCE

- **Access to NACCOP's annual 9 on IX webinar series at no additional cost (a \$710 value)**
 - These 60-minute succinct webinars will offer legal insight and practical guidance on Title IX topics from experts who have served or are currently serving as active practitioners on college and university campuses.
- **Alliance-Exclusive Professional Development Opportunities such as the Title IX & Equity Open House Discussion Series**
 - An Alliance-exclusive virtual open house will be held bi-monthly (every other month, 6 sessions annually) to engage with experts from NACCOP's partner organization, D. Stafford & Associates, as well as other invited guests, to discuss current trends and issues. Each open house will focus on a specific topic for discussion and participants will be encouraged to engage in the conversation.
- **Access to Alliance-Exclusive Whitepapers regarding Title VI, VII, and IX**
- **Connect and collaborate with other Title IX and Equity Professionals via an Alliance-restricted Listserv**
- **Discounted Professional Development Opportunities**
 - Coffee and Conversations webinar series and individual webinars focused on Title IX & Equity compliance issues
- **A 50% discount on the Title IX Notice Document Library developed by NACCOP's Partner Organization, D. Stafford & Associates (a \$335 value)**

Join the Alliance

Eligible individuals must have Institutional, Professional, or Committee Membership with NACCOP.

Cost: \$425 for 1 year subscription

(The first year of enrollment will be pro-rated to match the NACCOP membership expiration date.)

Request to Join: <https://naccop.memberclicks.net/join-the-alliance>

Questions? Contact us at info@naccop.org or 302-344-1068.