DELAWARE STATE BAR ASSOCIATION

CONTINUING LEGAL EDUCATION

Understanding the Next Frontier of Digital Communications and Forensic Collections

November 30, 2023, 12:00PM – 1:30PM

Live at the DSBA (Webcast in Georgetown & Dover)

DSBA WiFi Access

Sponsored by Parcels Inc.

1.5 Hours of CLE credit in Enhanced Ethics for Delaware and Pennsylvania Attorney

In the rapidly changing digital landscape, it's imperative to stay abreast of emerging technologies. The acquisition of content from trending data sources is crucial and must be done in a manner that's not only defensible but also meets the highest forensic standards. This approach is critical to steer clear of potential complications related to spoliation. We will hear from the Director of Digital Forensics, Scott Pearson of Parcels Inc. who is an expert in this field.

Visit www.dsba.org/cle or all the DSBA CLE seminar policies. Please note that the attached materials are supplied by the speakers and presenters and are current as of the date of this posting.

DELAWARE STATE BAR ASSOCIATION

Seminar Speaker:

Scott Pearson
Director of Digital Forensics / ISMS Lead
Parcels, Inc.

Visit www.dsba.org/cle or all the DSBA CLE seminar policies. Please note that the attached materials are supplied by the speakers and presenters and are current as of the date of this posting.

Scott Pearson

scott.pearson1@outlook.com • (973) 216-8055
www.linkedin.com/in/pearsonscott/ • Wilmington, DE, 19801

Director of Digital Forensics / ISMS Lead

Diligent and goal-focused manager experienced in defining direction/strategies for government agencies, as well as private firms.

Instrumental in implementing strategic procedures involving the forensic collection and analysis of ESI from multiple sources including cloud repositories, document collaboration platforms, mobile devices, computer systems, network servers, social media platforms, and the Dark Web in support of ongoing litigation. Demonstrated success in providing network-based and host-based incident response, while focusing on assessing cyber security position by identifying gaps and enterprise-level network security weaknesses to provide appropriate solutions. Remarkable efficiency in leading and mentoring multi-faceted teams on many cases both domestic and international, involving the forensic acquisition and analysis of digital evidence. Articulate communicator possessing excellent problem-solving and analytical skills with keen attention to detail.

Areas of Expertise

- Cybersecurity / Linux Security
- Risk Identification & Mitigation
- Critical Solutions & Consultations
- Digital Forensics Investigations
- Data Collection, Analysis & Interpretation
- Team Coordination & Leadership
- Staff Training & Development
- Performance Improvement
- Program Management

Technical Proficiencies

Platforms: X-Ways Forensics, Magnet Axiom, EnCase Forensic, Access Data FTK, Autopsy, Volatility, SIFT, Oxygen Forensics, Cellebrite UFED & Physical Analyzer, Apple Macintosh, Microsoft Windows, Microsoft Office 365, Google Workspace, Linux, X1 Social Discovery, Kali Linux, Tenable Nessus Pro, Nmap

Career Experience

Parcels, Inc. – Wilmington, DE **2020 – Present**
Director of Digital Forensics / ISMS Lead

As division lead, tasked with the creation and execution of technical solutions for a top eDiscovery/Litigation support service provider. Responsibilities include the forensic collection of electronically-stored information (ESI) from data custodians and the integration of gathered digital evidence into legal review platforms (i.e. RelativityOne). Routinely consult with lead counsel and law firm partners to implement strategies and ensure complex case requirements are met.

As ISMS Lead, oversee the security steering committee in charge of the creation, implementation, and careful maintenance of security policies, procedures, and guidelines, all to uphold the ISO 27001 certification. Successfully led transition from ISO 27001:2013 to ISO 27001:2022 standard.

San Diego State University | USSS National Computer Forensics Institute – San Diego, CA / Hoover, AL **2018 – Present**
Adjunct instructor | Lead Instructor

Conduct technical training sessions at the campus for students enrolled in the highly acclaimed Cybersecurity Professional Program. Act as a certifying instructor or the nationally recognized BCERT program, to deliver training in digital forensics to United States law enforcement, including Municipal Police, State Police, and Sheriff's Department, on behalf of the US Secret Service.

- Certified 100+ LE analysts in digital forensics and incident response on behalf of the US Secret Service for the highly selective BCERT program.

- Conducted regular consultations with major software and hardware commercial vendors on feature requests, overall functionality, and integrity of tools, focusing in digital forensics and incident response.
- Achieved over 90% matriculation into the Cybersecurity Professional program at San Diego State University and California State University Long Beach.

Digital Shield, Inc. – Palm Bay, FL **2015 – Present**
Consultant

Oversee and execute operations ranging from in-depth analysis and technical assistance to training and mentorship for foreign/domestic law enforcement and private entities on various aspects, such as forensic acquisition of digital evidence; digital forensics analysis (computer-based, network-based, mobile devices); network-based investigations; cybersecurity; vulnerability assessments; penetration testing, incident response; social media / dark web investigations; and course development / technical training on digital forensics, triage, incident response, Internet-based investigations, and cybersecurity. Coordinated with wide-ranging clients, including Virginia State Police – High Tech Crimes Unit; Northern Virginia Internet Crimes Against Children Task Force (ICAC); Southern Virginia Internet Crimes Against Children Task Force (ICAC); US DoS Anti-Terrorism Assistance Program; and CGH, Inc.

- Performed digital forensics of servers, workstations, mobile devices, and social media targets, submitted as evidence in high-profile cases for private sector clients.
- Assessed network security posture of private-sector clients, while coordinating with senior-level management for expediting the implementation of gaps identification and mitigation.

US Department of State Anti-Terrorism Assistance – Vienna, VA **2004 – 2020**
Consultant/Digital Forensic Analyst

Develop and deliver training curriculum for basic and advanced-level courses in DFIR and Network Security, while overseeing digital forensics, internet-based investigations, and cyber security on behalf of the US Dept of State to High-Tech Crime Units and digital forensic labs of Allied nations worldwide. Bolster productive relationships with foreign law enforcement and military personnel responsible to combat cyberterrorism. Organize and lead multiple teams into insurgent hot zones for aiding in design and establishing digital forensic labs for extracting evidence from computers and mobile devices seized as part of ongoing operations.

- Designed, developed, and delivered course development, technical training, and digital forensic lab mentorships to government analysts of over 35 Allied nations worldwide, including Pakistan, India, UAE, Egypt, Jordan, Kenya, Ethiopia, Morocco, Colombia, Paraguay, Mexico, Philippines, Thailand, Singapore, Jamaica, Trinidad and Tobago, Antigua, The Bahamas, Kazakhstan, Albania, Indonesia, Malaysia, Turkey, Brazil, and Oman.
- Consulted with US DoS Diplomatic Security agents on the DFIR capabilities of Allied nation operatives, such as foreign LE, Military, and private sector consultants, and overall network security posture of foreign LE agencies.
- Successfully led small team of cybersecurity analysts into Athens, Greece on behalf of the US DoS during the 2004 Summer Olympics to guide the Greek military analysts responsible for securing the Olympic Security Data Network (OSDN).

Additional Experience

US Department of Defense Computer Investigations Training Academy, Instructor - Linthicum, MD

Education

Master of Science in Cybersecurity
University of Delaware – Newark, DE

Bachelor of Arts in Information Systems
New Jersey Institute of Technology – Newark, NJ

Certifications

CompTIA Certified Information Systems Security Professional (CISSP) – *in progress*
IACIS Certified Forensic Computer Examiner (CFCE)
LPI Linux Essentials (LE-1)
US Secret Service National Computer Forensics Institute (NCFI) Certified Instructor, BCERT

Publications

Mastering Windows Network Forensics and Investigation, 2nd Edition
Published by Sybex Wiley

https://www.amazon.com/Mastering-Windows-Network-Forensics-Investigation/dp/1118163826

Understanding the Next Frontier of Digital Communications and Forensic Collections

CONTINUING LEGAL EDUCATION

Parcels

About me…

2003

Bellcore
Bell Communications Research

R
NJIT

US DoS

USSS

MSc Cybersecurity

Parcels

Digital Communications

- Traditional vs. Next Generation platforms
  - What data sources are your custodians utilizing?
    - **Hint:** it's not just Email and SMS!
- Forensic collections
  - Requirements
    - Date restrictions
    - Search terms - Good idea??
      - **Targeted:** in-place vs. in-line
  - Obstacles?
  - Deliverable – expectations vs. *reality*

Parcels

Traditional Platforms: **Email**

- How is it used?
  - Enterprise communications
  - Personal communications
  - Document archival
- Collection Challenges
  - Service provider
    - Personal vs. Enterprise
  - Remote collection vs. onsite
  - Modern authentication?
  - Data recovery
  - Obstacles

- Deliverable
  - PST – *one per custodian*
  - EML
  - MSG

Parcels

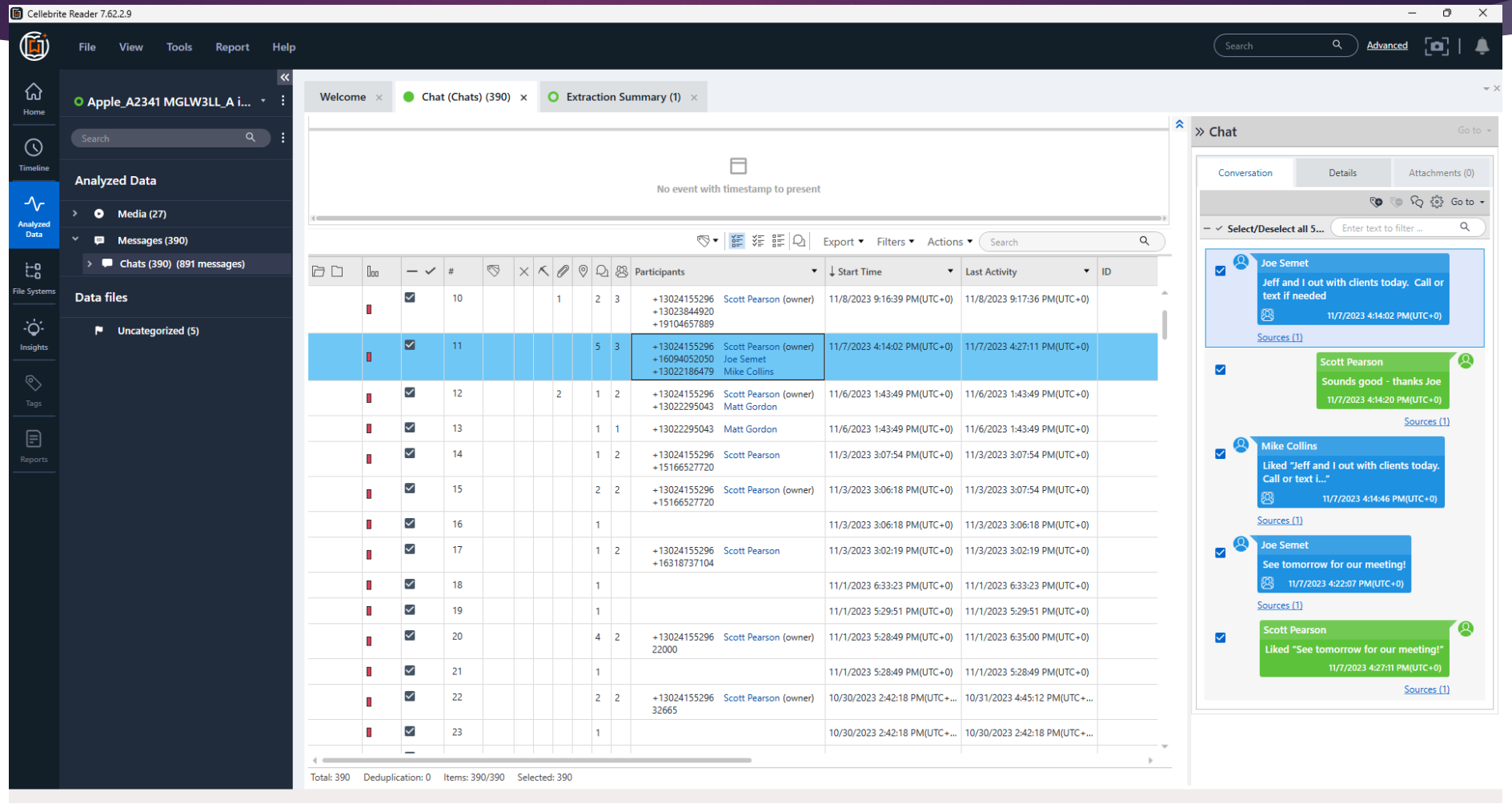
Traditional Platforms: **SMS**

- How is it used?
  - Text-based communications & MMS
  - Mobile Device specific – work/personal
- Collection Challenges
  - Device type & compatibility
    - iOS vs. Android
  - Searching in-place
  - Data recovery
  - Custodian self-collection

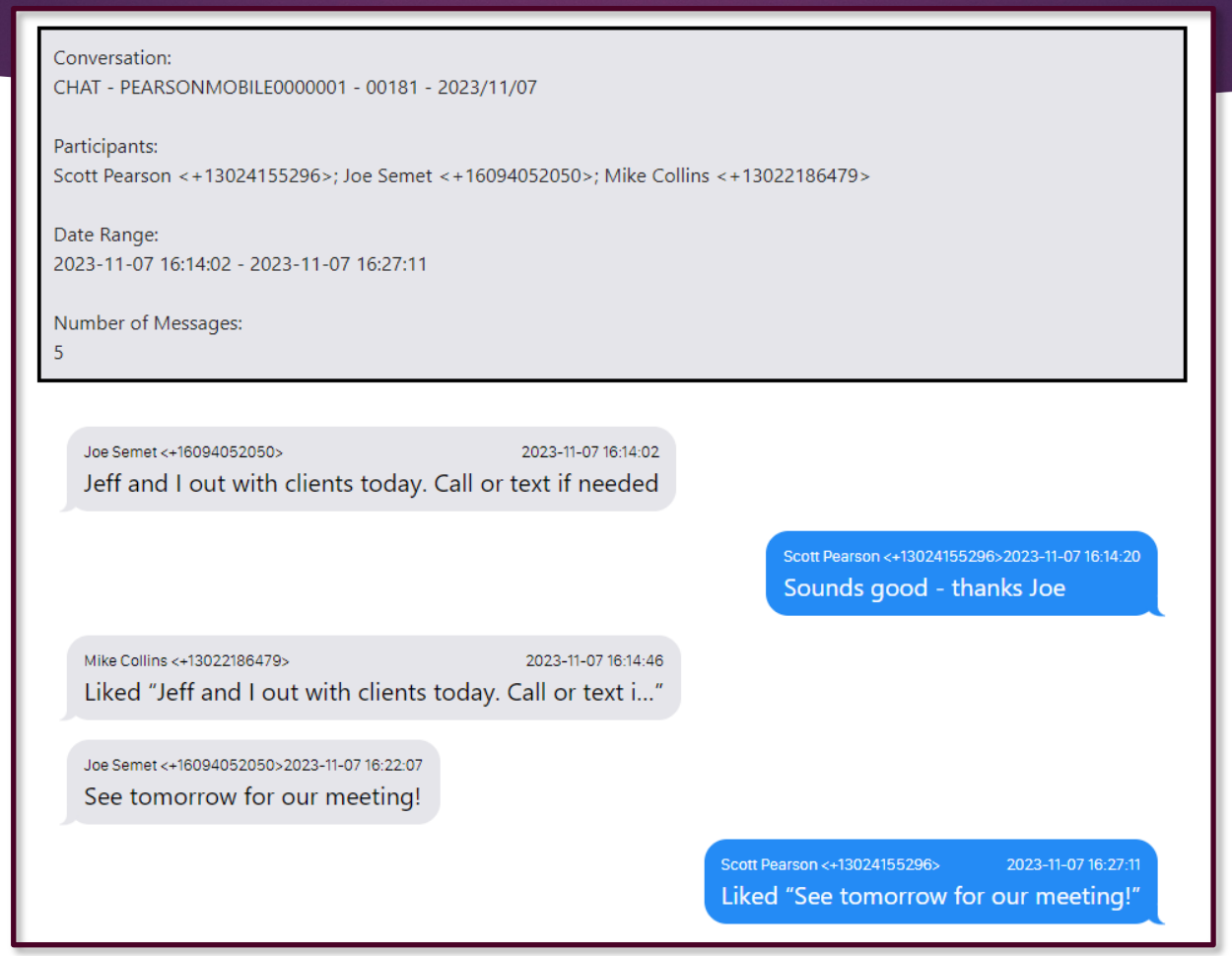
- Deliverable
  - RSMF – **huh??!**
  - Cellebrite UFDR
  - DAT / Concordance load file

Parcels

Cellebrite UFDR



Conversion to RSMF



Conversation:
CHAT - PEARSONMOBILE0000001 - 00181 - 2023/11/07

Participants:
Scott Pearson <+13024155296>; Joe Semet <+16094052050>; Mike Collins <+13022186479>

Date Range:
2023-11-07 16:14:02 - 2023-11-07 16:27:11

Number of Messages:
5

Joe Semet <+16094052050> 2023-11-07 16:14:02
Jeff and I out with clients today. Call or text if needed

Scott Pearson <+13024155296>2023-11-07 16:14:20
Sounds good - thanks Joe

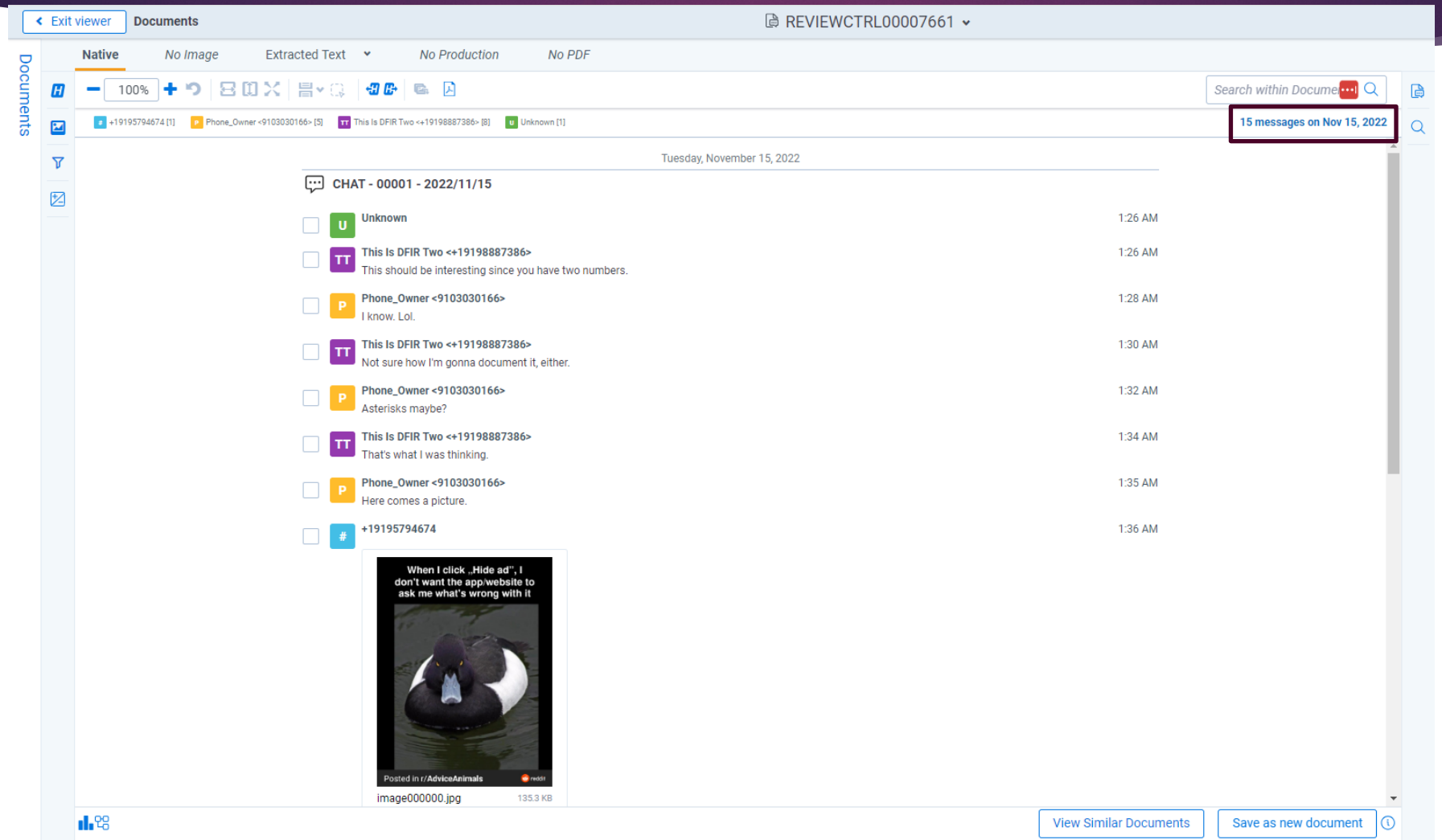
Mike Collins <+13022186479> 2023-11-07 16:14:46
Liked "Jeff and I out with clients today. Call or text i..."

Joe Semet <+16094052050>2023-11-07 16:22:07
See tomorrow for our meeting!

Scott Pearson <+13024155296> 2023-11-07 16:27:11
Liked "See tomorrow for our meeting!"

Preview

Relativity Short Message Format



- Conversation view
- 24-hour period
- Intuitive review
- De-duplication issues

Relativity one

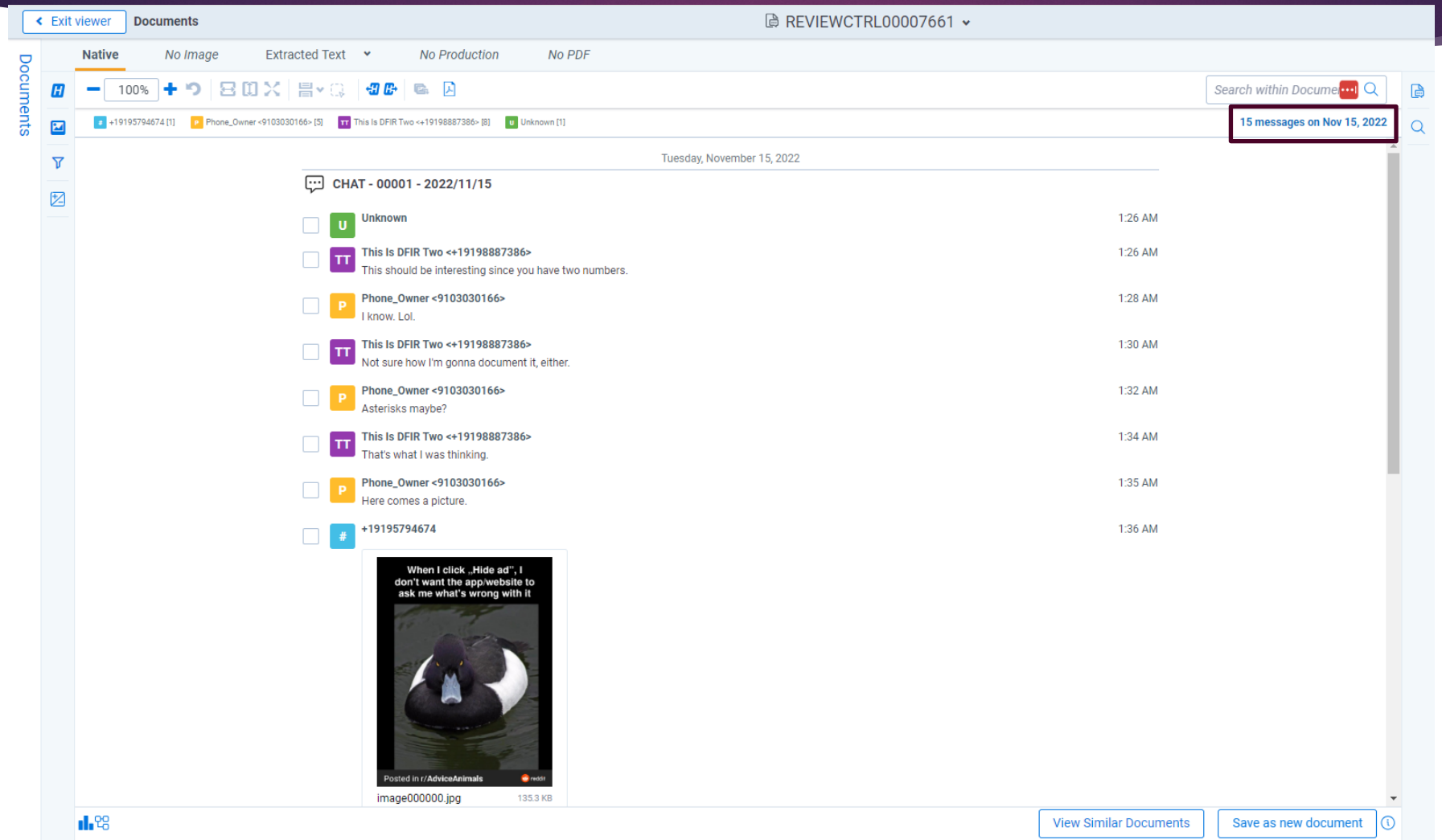
Next Generation Platforms: **Slack**

- How is it used?
  - Cloud-based enterprise communications – huh??
    - Internal / External
- Collection Challenges
  - Understanding subscription tiers and user roles
  - Data volume
  - API limitations
  - Searching in-place
  - Message retention

- Deliverable
  - RSMF
  - JSON (native)
  - DAT / Concordance load file

Parcels

Relativity Short Message Format



- ***Channel*** view
  - Workspace
  - DMs
  - Group DMs
- 24-hour period
- Intuitive review
- De-duplication

Relativity one

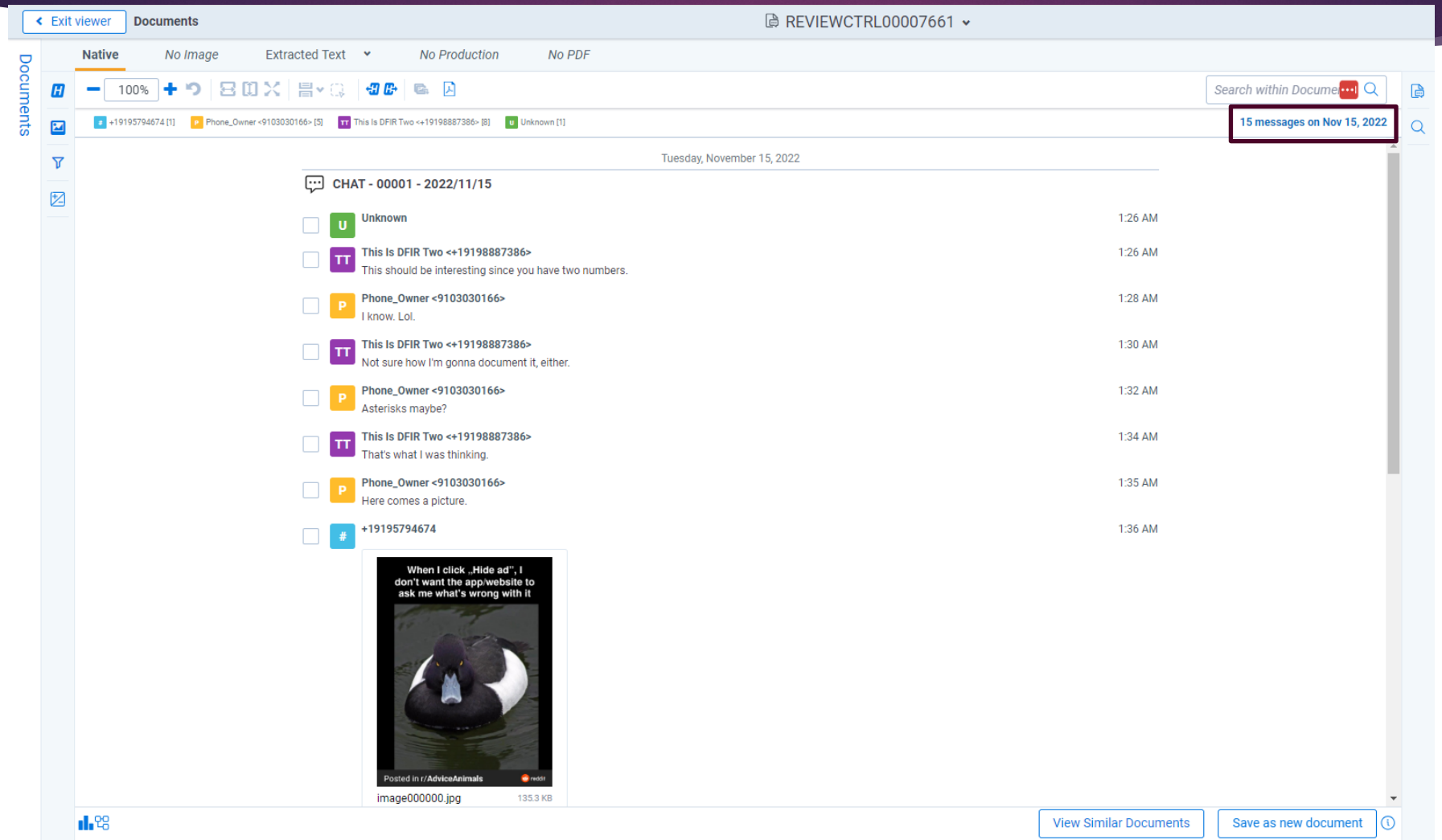
Next Generation Platforms: **Teams**

- How is it used?
  - Cloud-based enterprise communications
    - Internal and external
- Collection Challenges
  - Understanding Microsoft 365 Enterprise tiers
    - E1; **E3**; **E5**; F5; A1??
  - Navigating Microsoft Purview eDiscovery
  - Searching in-place
  - Message retention

- Deliverable
  - RSMF
  - PST
  - DAT / Concordance load file

Parcels

Relativity Short Message Format



- ***Teams*** view
- Conversation view
- 24-hour period
- intuitive review
- De-duplication

Relativity one

Next Generation Platforms: **Telegram**

- How is it used?
  - Cloud-based communications
  - Security
  - Anonymity
- Collection Challenges
  - Ephemeral
  - Device compatibility issues
  - Getting banned!
  - Managing platform identities
  - Encryption
  - Searching in-place

- Deliverable
  - RSMF
    - Public Channels
    - Private Channels
    - DMs
  - DAT / Concordance load file

Parcels

JavaScript Object Notation

```
{
 "name": "StarShip Official",
 "type": "private_supergroup",
 "id": 1830727601,
 "messages": [
  {
   "id": 60977,
   "type": "message",
   "date": "2023-10-03T01:29:19",
   "date_unixtime": "1696292959",
   "from": "Arina",
   "from_id": "user5091944775",
   "text": "Something strange with my wallet shows me I have 3lm token (another part sent to another wallet) but
   doesn't allow me to send them...says amount insufficient is this cause I haven't migrated yet",
   "text_entities": [
    {
     "type": "plain",
     "text": "Something strange with my wallet shows me I have 3lm token (another part sent to another wallet) but
     doesn't allow me to send them...says amount insufficient is this cause I haven't migrated yet"
    }
   ]
  },
```

Conversion to RSMF

Preview

Conversation:
StarShip Official - 2023-10-03

Participants:
Arina; Stuart; Vicky

Date Range:
2023-10-03 01:29:19 - 2023-10-03 19:14:55

Number of Messages:
4

Arina 2023-10-03 01:29:19
Something strange with my wallet shows me I have 31m token (another part sent to another wallet) but doesn't allow me to send them...says amount insufficient is this cause I haven't migrated yet

Stuart 2023-10-03 02:47:16
Use the migration steps Dorin , it's Easy and straight forward .

>>>scan the QR to connect wallet >>>>>approve smart contract > Click Add new contract button as custom token.

Stuart 2023-10-03 02:47:31
Complete the migration and try again

Vicky 2023-10-03 19:14:55
Migration done.Just waiting for the next bullrun

Next Generation Platforms: **Discord**

- How is it used?
  - Cloud-based communications
  - Community file sharing
  - Anonymity
- Collection Challenges
  - Understanding "guilds"
  - API limitations
  - Getting banned!
  - Server access restrictions (invite-only / admin)
  - Private guilds and DMs
  - Data volume
  - **No provisions for eDiscovery!**

- Deliverable
  - RSMF
    - Public guilds
    - Private guilds
    - Invite-only guilds
    - DMs
  - JSON (native)
  - DAT / Concordance load file

Parcels

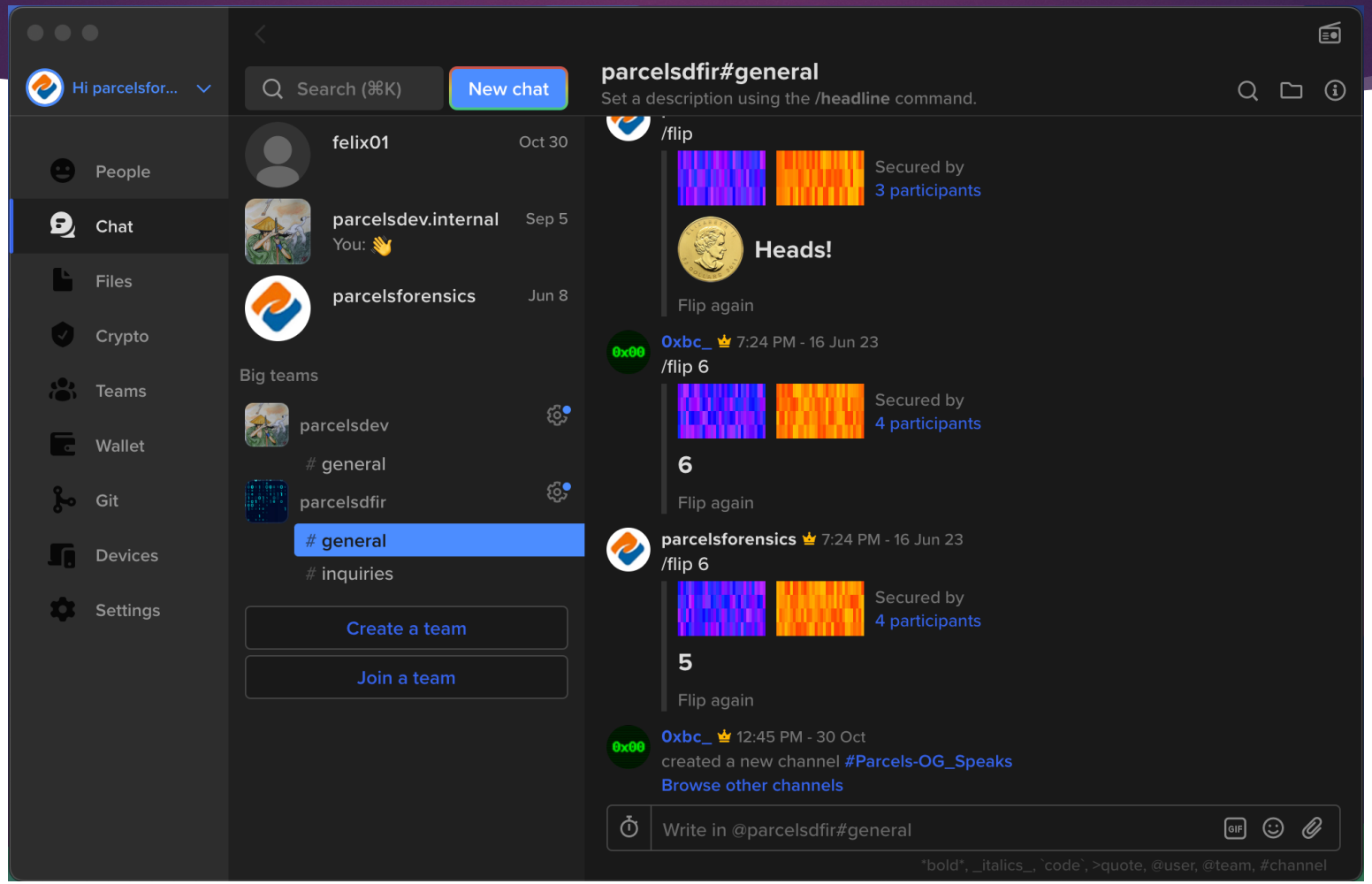
Next Generation Platforms: **Signal & Keybase**

- How is it used?
  - Secure communications
  - E2EE
- Collection Challenges
  - Encryption
  - Ephemeral
  - Forensic support
  - **No provisions for eDiscovery!**

- Deliverable
  - Screenshots…
  - Automated collection not reliable or *forensically sound*

Parcels

Secure Comms



Keybase

Next Generation Platforms: **X (formerly Twitter)**

- How is it used?
  - Community engagement
    - Politics
    - Trending topics
    - Cryptocurrency
  - Discrete communications
  - Anonymity
- Collection Challenges
  - Access restrictions
    - Protected accounts
    - Free vs. Premium
  - Data volume
  - ***some*** **provisions for eDiscovery**

- Deliverable
  - DAT / Concordance load file
  - Screenshots
  - RSMF
    - DMs only

Parcels

Concordance Load File

filename	collection_id	collected	date	type	text
OrkpQcbr2cSPLVSC-tweets-000001-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.253Z	2022-09-21T23:26:43.000	tweets	clearly unhappy with the current rate of nuking
OrkpQcbr2cSPLVSC-tweets-000001-b-photo-0001.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.434Z	2022-09-21T23:26:43.000	images	
OrkpQcbr2cSPLVSC-tweets-000002-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.304Z	2022-09-21T23:25:56.000	tweets	ask yourself why would sbf be raising a billy in this market? is ftx insolvent? is caroline blackmailing him? nah, they just need more money to keep shorting your coins
OrkpQcbr2cSPLVSC-tweets-000003-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.343Z	2022-09-21T23:17:14.000	tweets	web2 shareholders would never baghold for jpegs, only possible on web3
OrkpQcbr2cSPLVSC-tweets-000003-b-photo-0001.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.466Z	2022-09-21T23:17:14.000	images	
OrkpQcbr2cSPLVSC-tweets-000004-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.387Z	2022-09-21T22:54:53.000	tweets	i sold, sorry
OrkpQcbr2cSPLVSC-tweets-000005-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.422Z	2022-09-21T22:49:34.000	tweets	now this is a man who can make marke
OrkpQcbr2cSPLVSC-tweets-000005-b-photo-0001.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.526Z	2022-09-21T22:49:34.000	images	
OrkpQcbr2cSPLVSC-tweets-000005-b-photo-0002.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.508Z	2022-09-21T22:49:34.000	images	
OrkpQcbr2cSPLVSC-tweets-000006-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.471Z	2022-09-21T21:28:40.000	tweets	can anatoly restart eth plz?
OrkpQcbr2cSPLVSC-tweets-000007-a.png	OrkpQcbr2cSPLVSC	2022-09-22T14:40:29.507Z	2022-09-21T20:35:34.000	tweets	eth hit range highs and lows on dydx ke

Next Generation Platforms: **Instagram**

- How is it used?
  - Community engagement
    - Trending topics
    - Pop culture
    - Digital marketing
  - Discrete communications
- Collection Challenges
  - Access restrictions
    - Protected accounts
    - Direct messages
  - Data volume
  - **No provisions for eDiscovery!**

- Deliverable
  - DAT / Concordance load file
  - Screenshots
  - RSMF
    - DMs only

Parcels

Next Generation Platforms: **LinkedIn**

- How is it used?
  - Professional networking
    - Trending topics
    - Digital marketing
    - Recruiting / Headhunters
  - Research
- Collection Challenges
  - Access restrictions
    - Protected accounts
    - Direct Messages
  - Reach
  - ***some*** **provisions for eDiscovery!**

- Deliverable
  - DAT / Concordance load file
  - Screenshots
  - RSMF
    - DMs only

Parcels

What's Next?

- Compatibility with digital payment networks
  - Zelle, CashApp, Apple Pay, Google Pay, etc…
- Mass translation
- Enhanced message editing – *post send*
- AI bots
- Platform enhancements that encourage expression…and provide anonymity
  - Ex. non-unique display names

Parcels
Questions

Points of Contact

230 North Market Street, Wilmington, DE

- Scott Pearson, Director of Digital Forensics
  - spearson@parcelsinc.com
  - www.linkedin.com/in/pearsonscott
  - (302) 415-5296
- Joe Semet, Director of Business Development
  - jsemet@parcelsinc.com
  - www.linkedin.com/in/joseph-semet-5529102/
  - (609) 405-2050