IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Case No.: 1:19-CR-00018-ABJ

UNITED STATES OF AMERICA,

v.

ROGER J. STONE, JR.,

Defendant.

DEFENDANT ROGER STONE'S MOTION TO SUPPRESS

Defendant ROGER STONE, files this motion to suppress all evidence as fruit of illegal search warrants executed on specified dates and times. The warrants and applications are filed under seal.

BACKGROUND

The Government stated in its Opposition to Stone's Motion to Dismiss (Dkt # 99) that it will not be required to prove that the Russians hacked either the Democratic National Committee ("DNC") or Democratic Congressional Campaign Committee ("DCCC") from outside their physical premises or that the Russians were responsible for delivering the data to WikiLeaks. These assumptions formed the inadequate basis for the search warrants conducted in this case and the Indictment of Defendant. In addition to the fundamental assumptions, the government designated Roger Stone's case as related to *United States v. Netyksho et. al.* No. 18-cr-215 (ABJ) and cites to this Indictment in certain search warrant applications. (*See e.g.* Exhibit, Google search warrant application at 6, ¶18). If these premises are not the foundation for probable cause, Roger Stone communicating with a Twitter user named "Guccifer 2.0" or

speaking with WikiLeaks, would not constitute criminal activity.

Roger Stone has been charged with obstruction of Congress, lying to Congress, and witness tampering under 18 U.S.C. §§ 1505, 1001, 1512(b)(1), 2. The search warrant applications however, allege that the FBI was investigating various crimes at different times, such as Stone for accessory after the fact, misprision of a felony, conspiracy, false statements, unauthorized access of a protected computer, obstruction of justice, witness tampering, wire fraud, attempt and conspiracy to commit wire fraud, and foreign contributions ban. The uncharged conduct particularly relied upon the assumptions the Russian state is responsible for hacking the DNC, DCCC,[1] and even (although not as clear) Hillary Clinton campaign manager, John Podesta.

There is a certain forensic methodology that the FBI, Secret Service, or any other law enforcement agency conducting a computer forensic analysis follows. The first, and arguably most crucial step in the evidence gathering process, is to preserve the evidence. The imaging of the forensic data in its native format is key to preserving forensic evidence so as to allow agents to present authentic evidence in Court. Federal Rule of Evidence 902(14) permits authentication through a "process of digital identification by a qualified person" as long as it complies with Rule 902(11).[2] That Rule requires compliance with the business records exception of hearsay: "the record was made at or near the time by – or from information transmitted by someone with knowledge." Fed.R.Evid. 803(6)(a). Neither the Mueller report (from what we can tell), nor the CrowdStrike Reports (also heavily redacted) provide sufficient indicia of authenticity.

[1] WikiLeaks never released the DCCC documents. The Mueller report suggests the hack of the DCCC only provided additional keys to access the DNC servers. (Mueller Report at 38).

[2] "A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided." Fed.R.Ev.902(14) (Comm. note).

Based on the information available, the DNC either failed to alert the FBI about a major security breach of its systems, or the FBI chose not to respond to said breach. Consequently, the DNC hired a private company – CrowdStrike. It is also unclear if the FBI ever conducted a forensic analysis on the DCCC servers. It is clear, however, that the government has relied on the assumptions made by a source outside of the U.S. intelligence community that the Russian State was involved in the hacking and that the data taken from the various servers were given to WikiLeaks. The government cannot prove either since it did not participate in the investigation at the earliest stage. The government does not have the evidence, and it knew it did not have the evidence, when it applied for these search warrants. Now the government confesses: *"The Office cannot rule out that stolen documents were transferred to WikiLeaks through intermediaries who visited during the summer of 2016."* (Mueller Report at 47).

The government cites to CrowdStrike,[3] a private forensic computer firm, but not a government investigation through the FBI.[4] CrowdStrike's draft reports were provided to the defense, but not finalized reports, and they were heavily redacted. The first step in any computer fraud case is to encase and image the "attacked" computer. (Exhibit, DOJ Digital Forensic Analysis Methodology). CrowdStrike failed to encase the subject computers. This failure was fatal to any effort undertaken to ensure that investigation about whether the Russian government hacked the DNC, DCCC, or Podesta's computers was competent, thorough, and done by the

[3] CrowdStrike is not a government agency. It did not conduct its investigation at the behest of the government. The DNC and DCCC hired CrowdStrike to investigate the alleged theft of its data from its servers. (Indictment, ¶¶ 1-3). The CrowdStrike draft reports do not support its conclusions with evidence. In short, if this were an elementary school math problem, CrowdStrike not only does not show its work, it does not show the question – only its answer. Stone separately files a motion to compel an unredacted portion of the draft reports and any final reports. Stone also provides the draft reports of CrowdStrike under seal as Exhibits.

[4] CrowdStrike's three draft reports are dated August 8 and August 24, 2016. The Mueller Report states Unit 26165 officers also hacked into a DNC account hosted on a cloud-computing service on September 20, 2016, thereby illustrating the government's reliance on CrowdStrike even though the DNC suffered another attack under CrowdStrike's watch. (*See* Mueller Report at 49-50).

book. In fact, during Roger Stone's testimony to the House Permanent Select Committee on Intelligence, a squabble between members of Congress erupted over whether and when the FBI possessed the DNC's servers. (Exhibit, Tr. at 110-112).

Attached to this motion, as exhibits, are declarations from William Binney and Peter Clay. Both concur that in their opinions, WikiLeaks did not receive the stolen data from the Russian government. Their study and examination of the intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were delivered in a medium such as a thumbdrive. The data further indicates that the files were physically and manually acquired from the DNC inside the DNC office.

The *raison d'etre* of the Special Counsel's investigation was to pursue the claims that the Russians hacked and delivered the stolen data to WikiLeaks. (*See* Order appointing Special Counsel, Dkt. # 69-4). The foundation of all the search warrants was similar. If that foundation collapses, then the warrants must fail for lack of probable cause. Roger Stone requests this Court grant a *Franks* hearing for the reasons stated. The Court has already set aside June 21, 2019 for hearing time to discuss anticipated motions to suppress. Stone expressly requests an evidentiary hearing at that time. If the Court were to remove from the warrant applications, all the allegations that were speculation and are unproven or unprovable, then there would be no probable cause to support a search warrant for Roger Stone's papers, emails, cell phones, computers, and other devices.

MEMORANDUM OF LAW

Roger Stone is challenging the main underpinning of the search warrant applications supporting the warrants – the Russian government hacked the DNC, DCCC, and one Clinton Campaign official from locations outside where the computer servers were stored. *First*, Stone

will demonstrate that the Government's proposition is untrue. This assumption was not based upon a government investigation disclosed to the defense; rather, it was based upon CrowdStrike's, private investigation, of the respective servers of another private organization. *Second*, it appears those servers have not been encased and consequently, its data not properly preserved. The proper preservation is critical in order for it to be admissible at trial. Because of the failure of the Government to present proof in the search warrant applications, if the Court were to remove the misrepresentation from the warrant applications, no probable cause would exist to support the search warrants themselves. Stone is entitled to an evidentiary hearing to support his case, pursuant to *Franks v. Delaware*, 438 U.S. 154, 156, 98 S. Ct. 2674, 2676 (1978).

The Fourth Amendment provides in relevant part that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." *E.g. Collins v. Virginia*, 138 S. Ct. 1663, 1669 (2018). The Fourth Amendment requires a warrant supported by probable cause in order to support a lawful search. *Id.* Because there was a search warrant application drafted by government agents based upon the underlying assumption that the Russian state hacked the DNC, DCCC, and John Podesta's emails from the outside, the fruits of the search must be suppressed. *See, e.g., Wong Sun v. United States*, 371 U.S. 471, 484 (1963).

Franks requires the Court to evaluate: 1) was there a misrepresentation in the search warrant application; 2) was the misrepresentation reckless or worse; and, 3) if it there were misrepresentations, does the application for the warrant survive without the offending misrepresentations.

> We reverse, and we hold that, where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or

> with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.
>
> In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Franks, 438 U.S. at 155-56. *See also Pierce v. Mattis*, 256 F.Supp3d 7, 14 (D.D.C. 2017) (Berman Jackson, J.,).

The allegations in the warrant applications are nothing more than a collection of conclusory statements. There is no evidence, only supposition. This is not a substitute for factual allegations supporting probable cause.

> An affidavit in support of a warrant application "must provide the magistrate with a substantial basis for determining the existence of probable cause," and it cannot consist of "wholly conclusory statement[s]." *Illinois v. Gates*, 462 U.S. 213, 239, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).
>
> "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Id.* at 232, 103 S.Ct. 2317. The Supreme Court has recognized that the "task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that ... evidence of a crime will be found in a particular place." *Id.* at 238, 103 S. Ct. 2317 (abandoning the rigid two-prong test for determining informant veracity in favor of a totality of circumstances approach). Thus, a magistrate is supposed to consider the "totality-of-the-circumstances" in making probable cause determinations. *Id.*

United States v. Manafort, 313 F.Supp.3d 213, 228-29 (D.D.C. 2018). "Although we pay 'great deference' to the judge's initial determination of probable cause, a warrant application cannot rely merely on 'conclusory statement[s].'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (citations omitted). If this Court were to remove the language regarding the Russians hacking the DNC, DCCC, and Podesta, then the warrants lack probable cause. *See Franks*, 438 U.S. at 156 (removing offending portion of warrant and then evaluate probable cause); *United States v. Karo*, 468 U.S. 705, 719 (1984). If this Court were to remove the conclusory representations that the Russian state transferred the electronic data to WikiLeaks, there would be no probable cause to support the warrants. *See id.*

The indictment of Roger Stone is for obstruction of Congress, lying to Congress, and witness tampering; however, the purported crimes investigated and presented to the various courts reviewing the assorted warrants were much broader and were searching for a conspiracy between Stone, the Russians, or WikiLeaks. Because the two declarations provided to the Court debunks the underpinning of the warrants, Stone should be granted an evidentiary hearing. The government's agents knew that they could not prove the Russian state hacked the DNC or the other targeted servers, and transferred the data to WikiLeaks when it presented the search warrants to the various magistrates and district court judges.

CONCLUSION

This motion to suppress justifies an evidentiary hearing to which the Court has already set aside hearing time on June 21, 2019.

Respectfully submitted,

By: */s/*_____

L. PETER FARKAS
HALLORAN FARKAS & KITTILA, LLP
DDC Bar No.: 99673
1101 30th Street, NW
Suite 500
Washington, DC 20007
Telephone: (202) 559-1700
Fax: (202) 257-2019
pf@hfk.law

BRUCE S. ROGOW
FL Bar No.: 067999
TARA A. CAMPION
FL Bar: 90944
BRUCE S. ROGOW, P.A.
100 N.E. Third Avenue, Ste. 1000
Fort Lauderdale, FL 33301
Telephone: (954) 767-8909
Fax: (954) 764-1530
brogow@rogowlaw.com
tcampion@rogowlaw.com
Admitted pro hac vice

ROBERT C. BUSCHEL
BUSCHEL GIBBONS, P.A.
D.D.C. Bar No. FL0039
One Financial Plaza, Suite 1300
100 S.E. Third Avenue
Fort Lauderdale, FL 33394
Telephone: (954) 530-5301
Fax: (954) 320-6932
Buschel@BGlaw-pa.com

GRANT J. SMITH
STRATEGYSMITH, PA
D.D.C. Bar No.: FL0036
FL Bar No.: 935212
401 East Las Olas Boulevard
Suite 130-120
Fort Lauderdale, FL 33301
Telephone: (954) 328-9064
gsmith@strategysmith.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on May 10, 2019, I electronically filed the foregoing with the Clerk of Court using CM/ECF. I also certify that the foregoing is being served this day on all counsel of record or pro se parties, via transmission of Notices of Electronic Filing generated by CM/ECF.

BUSCHEL GIBBONS, P.A.

___/s/ Robert Buschel_____
Robert C. Buschel

United States Attorney's Office for the District of Columbia

Jessie K. Liu
United States Attorney
Jonathan Kravis
Michael J. Marando
Assistant United States Attorneys
Adam C. Jed
Aaron S.J. Zalinsky
Special Assistant United States Attorneys
555 Fourth Street, NW
Washington, DC 20530
Telephone: (202) 252-6886
Fax: (202) 651-3393

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

No. 19-cr-18 (ABJ)

ROGER J. STONE, JR.

Defendant.

DECLARATION OF WILLIAM E. BINNEY

I am William Binney and I hereby declare:

Background

1. I am a Cryptanalyst-mathematician.

2. I am a former employee of the National Security Agency ("NSA").

3. I was a Russia specialist and worked in the operations side of intelligence, starting as an analyst and ending as a Technical Director prior to becoming a geopolitical world Technical Director.

4. Between 1965 and 1969, I spent four years working in the U.S. Army Security Agency (the "ASA"). Until 1976, the ASA was the signals intelligence operation for the U.S. Army. Its mission was to intercept, acquire and decipher communications between persons, in electronic or any other form.

5. A true and correct copy of my resume is attached hereto as Exhibit 1.

6. After the Army, I spent 32 years working at the National Security Agency (the "NSA"). The NSA is the signals intelligence agency within the Department of Defense.

7. At the NSA, I held a variety of positions. These included the following positions:

2001 - Technical Leader, Intelligence

1999-2001 - Representative to the National Technology Alliance Executive Board
1996-2001 - Member of the Senior Technical Review Panel
1995-2001 - Co-founder/leader of the Automation Research Center (ARC)
2000-2001 - Technical Director of the Analytic Services Office
1998-2000 - Chair of the Technical Advisory Panel to the Foreign Relations Council
1998-2000 - Analysis Skill Field Leader, Operations
1997-2000 - Technical Director, World Geopolitical and Military
1996-1997 - Technical Director, Russia
1975-1996 - Leading analyst for warning, Russia
1970-1975 - Analyst on Russia

9. When I left the NSA in 2001, I was the Technical Leader for intelligence at the agency. As Technical Leader, I was the senior technical person in analysis at the NSA.

10. Prior to that, I was the Technical Director of the Analytical Services Office. In such position, I was responsible for handling all technical issues relating to the acquisition, development and distribution of signals intelligence for the agency's 6,000 analysts. These analysts were responsible for analysis and reporting for the entire world.

11. My duties included working with foreign governments who receive signals intelligence collected by the NSA. These include the so-called "Five Eyes" – *i.e.* the intelligence agencies for Australia, Canada, New Zealand, and the United Kingdom, in addition to the United States.

12. At the NSA, I was the primary designer and developer of a number of programs designed to acquire and analyze very large amounts of information and data files. The final program I was addressing dealt with the acquisition of information from the internet.

Opinions

13. WikiLeaks did not receive the stolen data from the Russian government.

14. Intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were delivered in a medium such as a thumbdrive.

physically local to the DNC.

Supporting Reasoning

16. Forensic Fingerprint - An anomaly of the DNC data on the WikiLeaks site is that all last modified date and time stamps end in an even number. This is a side effect of files that have been copied directly from a source system (such as a server) to a physical medium such as a thumbdrive. This is in contrast to files that have been copied from one server over the internet to another system as used by hackers (*i.e.* Linux).

17. Time signatures – Guccifer 2.0 posted (time stamped) files it reveals a time signature that allows us to calculate the speed the files was copied. As each file is copied from the source to the destination, the file is time stamped. All of the files constantly demonstrate they were copied at speeds massively greater than internet speeds. This data came from "Guccifer 2.0." Again, consistent with files copied directly and manually to a thumbdrive inside the building.

18. Missing day – The DNC files from WikiLeaks reveal that they were copied in three tranches, on May 23, 25, and 26; skipping the 24th. This would be more consistent with files that were being covertly copied when opportunities presented themselves, as opposed to a collection of files that had already been gathered and then transmitted as a collection to a destination such as WikiLeaks.

19. Time zone - While a weak indicator, it needs to be noted that the time zones of the files are more consistent with working hours in America rather than other sides of the globe.

I declare under penalty of perjury that the foregoing is true and correct. Executed in _____this _9th___ day of May, 2019.

William E. Binney

William E. Binney

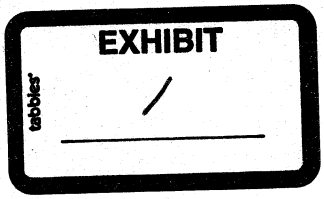
- Mathematician/Analyst -

Skill Areas: Intelligence Analysis; Traffic Analysis; Systems Analysis; Mathematics; Knowledge Management
Description of Most Recent Position

November 2005 - 30 June 2006 Entegra Systems Inc.
For the U.S. Customs and Border Protection, Office of Information Technology, Targeting and Analysis Systems Program Office, Mr. Binney defined statistical modeling techniques and advanced analytic processes, to support the modernization of CBP's Targeting and Analysis systems, tools, and analytical processes to perform predictive analysis of terror-related cargo and passenger transactions. Mr. Binney also supported the evaluation and integration of advanced analytic tools, both COTS tools and tools being develop by research universities and National Labs, under grants from the Department of Homeland Security, Advanced Research Projects Agency (HS/ARPA). Furthermore, Mr. Binney conducted an evaluation of CBP data quality, as well as defining techniques and processes for aggregating Cargo, Passenger, Law Enforcement, and Counter Terrorism-related data from multiple sources into a single, normalized entity-based repository.
Finally, Mr. Binney served as a member of a quick-reaction analytic team, which reviews available intelligence or information, and applies emerging advanced analytic technologies against selected operational data sets, to support executive level decision making and field operations.

Past Positions
From 2002 to 2004, as a member of Entity Mapping LLC., I worked on a contract for a major government organization. The contract effort centered on analysis of data to produce new entities and communities of interest. This effort required development of new data management processes, as well as analytic techniques to first verify the relationships between known entities of interest, then predict the existence of other entities of interest not previously observed. Our efforts also resulted in successfully developing a rules-based exclusionary approach that resulted in automatic discovery of newly observed but unpredicted entities of interest.

Positions held during 32 years career at the National Security Agency
2001 Technical Leader, Intelligence
1999-2001 Representative to the National Technology Alliance Executive Board
1996-2001 Member of the Senior Technical Review Panel
1995-2001 Co-founder/leader of the Automation Research Center (ARC)
2000-2001 Technical Director of the Analytic Services Office
1998-2000 Chair of the Technical Advisory Panel to the Foreign Relations Council
1998-2000 Analysis Skill Field Leader, Operations
1997-2000 Technical Director, World Geopolitical and Military
1996-1997 Technical Director, Russia
1975-1996 Leading analyst for warning, Russia



1970-1975 Analyst on Russia
Military service
1965-1969 Four years in the Army Security Agency (NSAICSS)

Career Experience:
Over the years, I, have applied mathematical, discipline to collection, analysis and reporting. In the process, I formulated Set Theory, Number Theory and Probability applications to collection, data analysis and intelligence analysis. Based on this experience, I was able to structure analysis, and transform it into a definable discipline making it possible to code and automatically execute these functions without human intervention from the point of collection to the end report. The successful automation of analysis formed the foundation for prototype developments in the ARC. These efforts caught the eye of Congressional Staffers and captured their imaginations. So much so that Congress actively supported and funded ARC development of automated systems. These systems revolutionized the business processes by demonstrating how to handle massive amounts of data effectively and relate results to military and other customers. I have also organized an international coalition of countries to jointly develop technology,. share results and gain the benefits of collaborative efforts. Primarily, I have focused on solving problems from a systems analysis perspective so that gains in any part of the business could be leveraged across the entire business enterprise.

Honors, awards and special achievements:
Directors Productivity Award - 1995
Technical Achievement Award - 1998
Gold Nugget Award - 1988
Numerous Letters of Appreciation Numerous cash awards

Degrees and Certificates:
B. S. Mathematics, The Pennsylvania State University, 1970 Certified Analysis Professional - 1973

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

No. 19-cr-18 (ABJ)

ROGER J. STONE, JR.

Defendant.

_____/

_____

DECLARATION OF PETER CLAY

I am Peter Clay and I hereby declare:

Background

1. I am an internationally experienced cyber security executive and senior advisor with 23 years of service to the world's largest private and public-sector entities, small to mid-sized organizations, US legislative and executive branches, and regulatory agencies.

2. Over my career I have worked with and for International Banks, State and Local Governments, the U.S. Navy, U.S. Mint, Department of Defense, Department of Homeland Security, General Services Administration, and Small Business Administration.

3. A true and correct copy of my *curriculum vitae* is attached as an Exhibit.

4. The below expresses my opinions and my reasoning is set out after the opinions. The reasoning is based upon publicly available documents from WikiLeaks.

Opinions

5. Given the information that is available it is more likely that the data posted to Wikileaks was removed by someone with physical access to the computing equipment rather than removal by an external actor.

6. Intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were most likely delivered in a medium such as a thumbdrive.

7. The data indicates that the files were likely acquired from the DNC manually and physically local to the DNC.

Supporting Reasoning

8. Forensic Fingerprint - An anomaly of the DNC data on the WikiLeaks site is that all last modified date and time stamps end in an even number. This is a side effect of files that have been copied directly from a source system (such as a server) to a physical medium such as a thumbdrive. This is in contrast to files that have been copied from one server over the internet to another system as used by hackers (*i.e.* Linux).

9. Time signatures – On the Guccifer 2.0 posted (time stamped) files it reveals a time signature that allows us to calculate the speed the files was copied. As each file is copied from the source to the destination, the file is time stamped. All of the files constantly demonstrate they were copied at speeds significantly greater than internet speeds. This data came from "Guccifer 2.0." Again, consistent with files copied directly and manually to a thumbdrive inside the building.

10. Missing day – The DNC files from WikiLeaks reveal that they were copied in three tranches, on May 23, 25, and 26; skipping the 24th. This would be more consistent with files that were being covertly copied when opportunities presented themselves, as opposed to a collection of files that had already been gathered and then transmitted as a collection to a destination such as WikiLeaks.

11. Time zone - While a weak indicator, it needs to be noted that the time zones of the files are more consistent with working hours in America rather than other sides of the globe.

12. From the information that has been provided it appears likely that standard forensic techniques regarding the preservation of the hard drives and volatile memory were not followed which leaves only the review of publicly available information as the forensic source.

I declare under penalty of perjury that the foregoing is true and correct. Executed in _____this _9th___ day of May, 2019.

Peter Clay

Peter Clay CISSP

cpthuah36@gmail.com · www.linkedin.com/in/peclay · m: 703-220-3531

Professional summary

Leader, advisor, mentor, strategist and experienced executive in the field of information security with a proven record of building security programs or consultancies and executing either on a global scale. Passionate about the role of security as both a protective and enabling function within the enterprise and skilled at delivering market beating results and capabilities. Experienced leading an internal CISO function, an external consultancy or participating in the development of new security tools and methodologies as a single practitioner.

Internationally experienced cyber security executive and senior advisor with 23 years of service to the world's largest private and public-sector entities, Fortune 1000's, small to mid-sized organizations, US legislative and executive branches, and regulatory agencies.

Summary of skills

- Leadership - startups to large multinationals
- M&A due diligence and integration
- Enterprise security design and architecture
- Managed Security Services Provider (MSSP)
- Network Intrusion Detection Systems (NIDS/NIPS)
- Host Intrusion Prevention Systems (HIDS/HIPS)
- Network Security Monitoring (NSM)
- Security Operations Centers (SOC)
- Event Correlation and Log Aggregation (SEM)
- Integrated security monitoring solutions (SEIM)
- Network and host forensic analysis
- Anti-virus/malware enterprise solutions
- Computer incident response (CIRT/CSIRT)
- Business Continuity/Disaster Recovery (BC/DR)
- Policy development and enforcement
- Enterprise vulnerability assessment systems
- PKI/digital rights management solutions
- Security Intelligence Fusion Centers
- Strategy and management consulting
- Security Analytics and Operations
- System development lifecycle
- Regulatory compliance (FISMA, SOX, DFAR, PCI)
- Privacy compliance (Privacy Act, GDPR)
- IT Governance (NIST, DOD, CobIT, ITIL)
- Cross functional collaboration
- Intellectual property control methods
- Security evangelism/client engagement
- Technology project management
- Executive briefings and presentations
- Security strategies and roadmaps
- Training development and delivery
- Venture integration/M&A analysis
- Enterprise risk management

Career summary

COO	Dark3	2019-Present
Owner	Fenris	2002 – present
Partner	Small Federal Consultancy	2016 – 2018
CISO	Qlik	2015 –2016
CISO	Invotas	2014 – 2015
Director II/CISO Fed Practice	Deloitte	2010 – 2014
Senior Manager	Deloitte & Touché LLP	2005 – 2010
Senior Manager	Urbach, Hacker, Young	2002 – 2004
Partner	CoDevelop	1995 – 2002

Certifications and Education

- Hendrix College (1985)
- Oxford University (1983)
- Certified Information Systems Security Professional (CISSP)
- Top Secret DoD Clearance
- Bachelor of Arts
- Junior Year Abroad Program
- Member, ISC^2

Professional experience

Fenris, *Charlottesville, VA* 2002 – present

Founder

Strategic advisor and independent expert in the fields of cyber security, managed services, regulatory compliance, and virtual CISO services. Specialized in supporting small to mid-sized enterprises (SME) implement, design, manage and operate their information security programs efficiently and effectively while meeting their compliance and reporting obligations.

Automated Financial Systems *New York, NY* 2002-2010

Managed Security Services

Retained to develop and deliver a complete managed security solution to the pioneer in online stock and commodities trading. Services included network/host intrusion detection, firewall management, incident response, PKI design, vulnerability management, security architecture and compliance reporting (NYSE/AMEX exchange requirements). Resulted in compliant security operations and identified as a key factor in winning bids on over $15 mm in new business.

Potlatch Timber Products *Warren, AR* 2004

Lead Security Architect, Industrial Controls

Developed and delivered secured industrial control solution that enabled remote vendor support via modem to 16 machine centers located in Central Arkansas. Identified as reducing major machine center downtime by over 74% and contributed to increasing over all mill throughput by 7% year over year.

Katzcy *Reston, VA* 2018

Virtual CISO

Retained to develop and implement company and product strategy for Katzcy's compliance with NIST 171 requirements in support of their Department of Defense contractor support. Designing the technology stack, completing the risk assessment, security plan and disaster recovery documentation while performing the continuous monitoring function and documenting the results.

ZTP *Rosslyn, VA* Sep 2016 – June 2018

Partner

Joined the partnership to develop the federal practice business pipeline, develop unique offerings for the federal and commercial markets and mentor the in-house security talent and identify additional talent that could add value to our operations. In 18 months with ZTP led the capture of over $70M in new federal business and helped the company expand into 3 new federal clients. Additionally, led the development of a commercial small to mid-sized business focused managed security practice that was recently selected by a global insurance company to be their exclusive go to market partner for a global launch by pairing their small business insurance products with ZenOpz managed technology stack.

ZTP Client engagements:

Small Business Administration *Washington, DC* Sep 2016-June 2018

Managed Security Services

Retained to develop and deliver complete security program support to the entire agency to include build a Security Operations Center from scratch, support over 30 authorization and accreditation packages annually, provide all security engineering, provide security intelligence functions and processes, be the key resource for disaster recovery and business continuity operations, perform all vulnerability management functions, provide key support for patch management, provide user training for over 6000 employees and enterprise wide penetration testing. During my tenure the scale of the program more than doubled and revenue jumped from $3.5mm to over $10 mm per annum.

General Services Administration, *Washington DC* Sep 2016-June 2018

Subject Matter Expert

Supported the accreditation and testing processes of ten vendors on a government wide contract to provide internet and networking services across the federal government. Developed a streamlined approach to performing the testing processes necessary for the accreditation and worked with the government selected vendors to prepare their documentation for submission and testing. Results of the streamlined testing efforts resulted in a follow-on award of over $2mm for FY 2019 to continue program support.

ZTP Commercial *Charlottesville, VA* Sep 2016-June 2018

Founder/Lead Architect

Developed a small business focused outsourced security program offering based on open source/free software designed to provide small to mid-sized organizations with the ability to execute a full security program in support of their specific compliance and data protection requirements. Developed and documented the 360-review process which married Risk Assessment, Security Maturity Model, Threat Matrix and Vulnerability assessments to provide a holistic view of the client's information security posture. Designed and built the tech stack supporting the process to make maximum use of automation/orchestration to reduce the headcount required to provide the operational support. Was selected over 3 national vendors as a go to market partner with a national education tech company with 1400 clients in the US and selected by an international insurance vendor as the launch partner for a global re-launch of their cybersecurity insurance product lines.

Qlik, *Philadelphia, PA* May 2015-Sep 2016

Chief Information Security Officer

As the first CISO hired by Qlik and the senior security practitioner on staff, I implemented the initial information security program at Qlik by rapidly creating cyber and data protection capabilities using limited staff and very limited financial resources. At the end of the first year the Qlik security program was protecting the primary assets of a software company operating in 32 countries globally.

- Stood up a combined operations/security Global Operations Center to provide a consolidated monitoring/triage function for the global network to include building 28 playbooks to support entity requirements in the first 6 months of operation
- Implemented entity wide security policies and procedures
- Managed 2 cycles of SOX 404 review successfully mitigating multiple findings from previous reviews
- Supported the re-architecting of the Salesforce solution to include minimal required security controls
- Supported federal sales by leveraging relationships and experience to manage federal security requirements for cloud and on prem solutions
- Implemented the first vulnerability management program in corporate history
- Designed, developed and led the CSIRT capability for the company
- Developed and supported the re-architecting of the global network to increase security of critical assets and reduce bottlenecks and single points of failure across the globe
- Created and evangelized a cyber governance model to leveraging open source tools and capabilities to rapidly increase the security maturity of the program
- Maintained active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners in support of issues and requirements

Invotas, *Alexandria VA* May 2014 – May 2015

CISO, Consulting Lead

As the client facing cyber security leader for Invotas my duties included securing our cloud-based/on premise orchestration engine, documenting our security environment, interfacing with clients regarding our risk management practices for the commercial and classified efforts and managing the development of the consulting and sales engineering group. Additionally, I was designated one of the thought leaders and authors for the company and worked with the marketing group to deliver timely articles and thought pieces to industry publications, manage interviews with national press and speak on a variety of topics at international security programs in the US, UK and UAE.

- Primary input into the development and operational requirements for the software products
- Responsible for developing the standardized "playbooks" for client use to include: endpoint, network and application incident response, automation supporting security intelligence enrichment functions, automated reporting and analysis capabilities, secure environment maintenance and integration with multiple classes of tools to include SEM, SIEM, Firewall, Router, HID, NID, Intelligence applications, endpoints and applications
- Delivered over 40 in person presentations ranging from keynote at a regional conference to small groups internationally (US, Europe, Middle East)
- Developed and evangelized original end-to-end company security strategy to integrate enterprise, product, and customer security objectives as a continuous cyber maturity model
- Architected and led global cyber governance and standardization efforts to align processes with applicable NIST, DOD and ISO requirements
- Led a multinational team of cyber security professionals and delivered security and sales engineering services globally
- Created and evangelized a cyber governance model to leverage automation and orchestration investment in cyber security initiatives for our clients
- Active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners to enhance orchestration awareness, capabilities, and training to US intelligence entities

Deloitte LLP, *Rosslyn, VA* Feb 2010 – May 2014

Chief Information Security Officer Deloitte Federal Practice

Developed and implemented a separate federally compliant computing environment that enabled the 8000 federal practitioners to operate without changing their hardware or computing environments. In addition, the Federal CISO team developed a federal cloud offering that provided the federal practice with the ability to leverage federally compliant infrastructure, platform and applications as a service and include those offerings to federal clients. The success of the federal program resulted in the transfer of the Federal Practice CISO team to the US Firms Information Risk and Compliance Group where I was rapidly promoted from Senior Manager to Director II and took on additional responsibilities to include firm wide security architecture and leadership of IRC.

- Reduced compliance efforts and requirements managed by the US firm from over 300 to 2 (FISMA/Firm global requirements)
- Responsible for securing ~60,000 personnel (on 4 continents) and 35% share of Deloitte's global $28B and 210,000- employee enterprise environment
- Restructured and led M&A Cyber Due Diligence and Remediation Program to enable accelerated integration of 19 acquired environments through risk-based assessment and remediation model
- Architected and oversaw deployment of a $12M global enterprise SIEM solution
- Architected and oversaw deployment of a $2M global Data Loss Prevention Solution
- Established US Firm's PKI infrastructure and deployed it to over 18 countries in 8 months
- Provided strategic guidance in development, deployment and use of a custom internally-developed SEM/DLP/Backup solution designed for real-time forensic analysis and incident response support
- Responded to every major intrusion incident on Deloitte's networks worldwide from 2010-2014
- Architected and deployed a FEDRAMP certified solution in support of Deloitte's federal practice that included Infrastructure, Platform and Application components in 4 months
- Oversaw PCI-DSS implementation for an 800-room hotel/training center
- Active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners to enhance threat intelligence awareness, defensive capabilities, and maturity benchmarking of the firm's cyber efforts as part of a long-term continuous improvement plan
- Developed & delivered award winning security training programs to train over 60,000 users annually using computer-based training, phishing exercises, customized training and executive briefing series on cybersecurity
- Rated in the top 10% of my peers throughout my tenure at Deloitte LLP

- Directly involved with over 80 interactions with F100 customers, partners, Federal and State CISO/CIO/CEO level

Deloitte & Touché LLP, *Rosslyn, VA* Aug 2005 – Feb 2010

Senior Manager

Hired as the 16th member of the Deloitte & Touché LLP Enterprise Risk practice and over the course of 4.5 years was integral to the capture of $65M in revenue at 6 different executive agencies, developed multiple federally focused processes (penetration testing, continuous compliance, risk management) still in use today and was part of the leadership team that delivered 400% growth over my tenure. Additionally, developed relationships with multiple software vendors to increase federal and commercial opportunities. Consistently rated in the top 25% of my peers in annual reviews.

Deloitte & Touch LLP Client Engagements:

Department of Homeland Security (DHS), *Crystal City, VA* 2008–2010

Senior Enterprise Risk Team Lead

- Designed and implemented the reference and solution architecture for the initial cloud environment to facilitate intelligence sharing between multiple agencies
- Supported the design and implementation of security processes for 8 agency wide applications
- Oversaw the authorization and accreditation process for multiple federal environments through a team of ISSO's
- Participated in developing formal feedback for DHS response to NIST regarding Special Publication 800-53
- Participated in developing the DHS policy regarding the accreditation of third party applications

World Bank, *Washington, DC* 2009

Penetration Test Lead

- Performed a series of penetration tests versus World Bank environments
- Developed the executive report deliverables and presented them to client leadership
- Architected the ongoing testing program on behalf of World Bank

Department of Defense, *Washington, DC* 2006-2008

IT Audit Lead

- Led multiple IT audits of general computer controls and technical configurations on behalf of DoD Inspector General with a team composed of Deloitte and contractor personnel
- Performed analysis of technical configurations and architectures throughout DoD in accordance with DoD instructions
- Developed recommendations for architecture, configuration and operational improvements
- Primary author of 4 DoD IG reports on various DoD applications

United States Mint, *Washington, DC* 2006-2007

IT Audit Lead

- Led the initial reviews performed in accordance with OMB A-123 (SOX for the federal government)
- Reviewed 6 Mint locations simultaneously with multiple teams of auditors and information security professionals
- Completed the time compressed project in 75% of the allotted time resulting in a government savings of over $1.2M in the first year
- Examined 30+ mission-critical business applications and functional components
- Audited critical infrastructure services: SIEM, Endpoint, Logging, Incident Response
- Determined compliance state at component, application, and functional levels

Urbach, Hacker, Young LLC *Washington, DC*

Senior Manager

Hired as the deputy leader of the IT Audit and Security team to provide leadership to multiple Navy Inspector General Audits and develop methodologies to support the growth of the IT security practice. Doubled the size of the practice in two years and created three new lines of business to support penetration of the commercial and federal markets.

UHY LLP Client Engagements:

Navy IG, *Washington DC* 2002-2004

Team Lead

- Led multiple reviews of Navy applications spanning global operations to include payroll, logistics, training and infrastructure systems
  - Deployed teams globally to perform local testing processes
  - Completed 100% of reviews on time and on budget
  - Examined 10+ applications and processes by determining compliance state at component, application and functional levels
  - Performed initial penetration testing in support of Navy IG Audits

New York Counties, *New York* 2002

Team Lead

- Led HIPAA reviews for hospitals in 9 New York counties
- Completed 100% of reviews on time and on budget
- Developed a data discovery and analysis technique that created significant operational efficiencies
- Used the operational efficiencies to expand the scope to include additional testing services in support of hospital disaster recovery plans

Deutsche Bank, *Global* 2004

Security Engineer/Architect

- Planned, architected and trained 6 travel teams on the Securify application for deployment throughout Deutsche Bank's global environment
- Managed all aspects of 6 simultaneous implementations every week for 5 weeks for a total of 30 installations on 6 continents
- Developed the formal documentation and "playbook" for deploying the Securify application along with the initial

CoDevelop, *Charlottesville, VA* 1995 – 2002

Partner

General Partner in CoDevelop an internet incubator located designed to identify very early stage companies and provide them with the resources necessary to realize the value of their concepts. Developed the 5-50-500 strategy which allowed companies to rapidly develop from a "back of the napkin" stage to effective market entry and a candidate for institutional investment. Provided operational leadership and mentorship to the early stage companies and successfully helped 4 of the companies to exit the program

Computer Forensics: Digital Forensic Analysis Methodology

Ovie L. Carroll
Stephen K. Brannon
Thomas Song
Cybercrime Lab,Computer Crime and Intellectual Property Section, Criminal Division
United States Department of Justice

Introduction

In comparison to other forensic sciences, the field of computer forensics is relatively young. Unfortunately, many people do not understand what the term computer forensics means and what techniques are involved. In particular, there is a lack of clarity regarding the distinction between data extraction and data analysis. There is also confusion about how these two operations fit into the forensic process. The Cybercrime Lab in the Computer Crime and Intellectual Property Section (CCIPS) has developed a flowchart describing the digital forensic analysis methodology. Throughout this article, the flowchart is used as an aid in the explanation of the methodology and its steps.

The Cybercrime Lab developed this flowchart after consulting with numerous computer forensic examiners from several federal agencies. It is available on the public Web site at www.cybercrime.gov/forensics_gov/forensicschart.pdf. The flowchart is helpful as a guide to instruction and discussion. It also helps clarify the elements of the process. Many other resources are available on the section's public Web site, www.cybercrime.gov. In addition, anyone in the Criminal Division or U.S Attorneys' offices can find additional resources on the new intranet site, CCIPS Online. Go to DOJ Net and click on the "CCIPS Online" link. You can also reach us at (202) 514-1026.

Overview of the digital forensics analysis methodology

The complete definition of computer forensics is as follows: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of

facilitating or furthering the reconstruction of events found to be criminal." A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop (DFRWS), available at http://dfrws.org/2001/dfrws-rm-final.pdf.

Defining computer forensics requires one more clarification. Many argue about whether computer forensics is a science or art. United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005) ("Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science."). The argument is unnecessary, however. The tools and methods are scientific and are verified scientifically, but their use necessarily involves elements of ability, judgment, and interpretation. Hence, the word "technique" is often used to sidestep the unproductive science/art dispute.

The key elements of computer forensics are listed below:

- The use of scientific methods
- Collection and preservation
- Validation
- Identification
- Analysis and interpretation
- Documentation and presentation

The Cybercrime Lab illustrates an overview of the process with Figure 1. The three steps, Preparation/Extraction, Identification, and Analysis, are highlighted because they are the focus of this article..

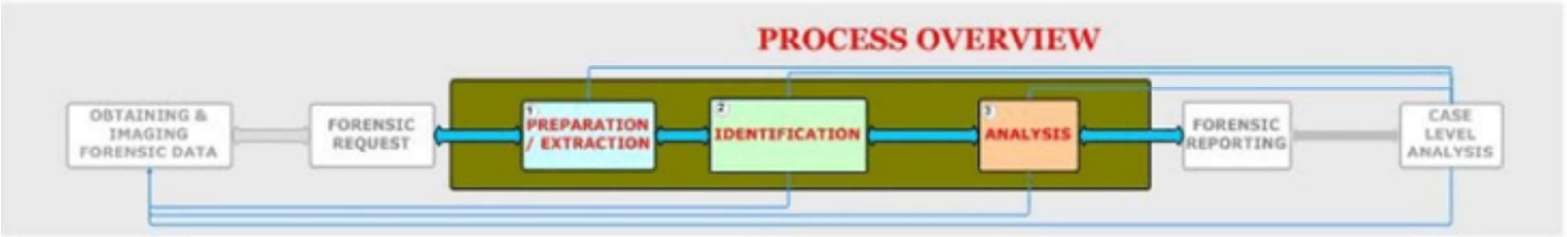


Figure 1

In practice, organizations may divide these functions between different groups. While this is acceptable and sometimes necessary, it can create a source of misunderstanding and frustration. In order for different law enforcement agencies to effectively work together, they must communicate clearly. The investigative team must keep the entire picture in mind and be explicit when referring to specific sections.

The prosecutor and forensic examiner must decide, and communicate to each other, how much of the process is to be completed at each stage of an investigation or prosecution. The process is potentially iterative, so they also must decide how many times to repeat the process. It is fundamentally important that everyone understand whether a case only needs preparation, extraction, and identification, or whether it also requires analysis.

The three steps in the forensics process discussed in this article come after examiners obtain forensic data and a request, but before reporting and case-level analysis is undertaken. Examiners try to be explicit about every process that occurs in the methodology. In certain situations, however, examiners may combine steps or condense parts of the process. When examiners speak of lists such as "Relevant Data List," they do not mean to imply that the lists are physical documents. The lists may be written or items committed to memory. Finally, keep in mind that examiners often repeat this entire process, since a finding or conclusion may indicate a new lead to be studied.

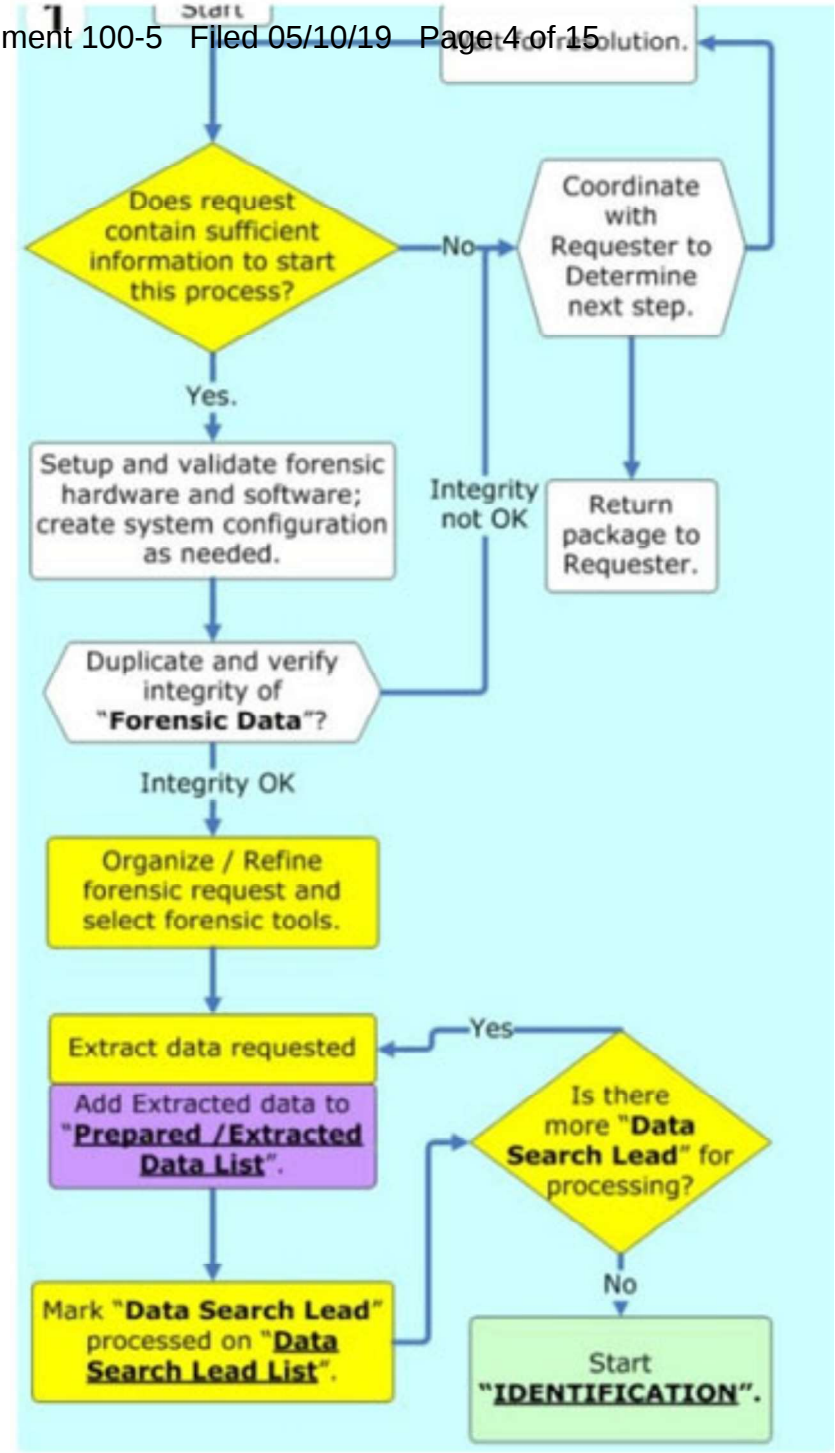
Preparation/Extraction

Examiners begin by asking whether there is enough information to proceed. They make sure a clear request is in hand and that there is sufficient data to attempt to answer it. If anything is missing, they coordinate with the requester. Otherwise, they continue to set up the process.

The first step in any forensic process is the validation of all hardware and software, to ensure that they work properly. There is still a debate in the forensics community about how frequently the software and equipment should be tested. Most people agree that, at a minimum, organizations should validate every piece of software and hardware after they purchase it and before they use it. They should also retest after any update, patch, or reconfiguration.

When the examiner's forensic platform is ready, he or she duplicates the forensic data provided in the request and verifies its integrity. This process assumes law enforcement has already obtained the data through appropriate legal process and created a forensic image. A forensic image is a bit-for-bit copy of the data that exists on the original media, without any additions or deletions. It also assumes the forensic examiner has received a working copy of the seized data. If examiners get original evidence, they need to make a working copy and guard the original's chain of custody. The examiners make sure the copy in their possession is intact and unaltered. They typically do this by verifying a hash, or digital fingerprint, of the evidence. If there are any problems, the examiners consult with the requester about how to proceed.

After examiners verify the integrity of the data to be analyzed, a plan is developed to extract data. They organize and refine the forensic request into questions they understand and can answer. The forensic tools that enable them to answer these questions are selected. Examiners generally have preliminary ideas of what to look for, based on the request. They add these to a "Search Lead List," which is a running list of requested items. For example, the request might provide the lead "search for child pornography." Examiners list leads explicitly to help focus the examination. As they develop new leads, they add them to the list, and as they exhaust leads, they mark them "processed" or "done."

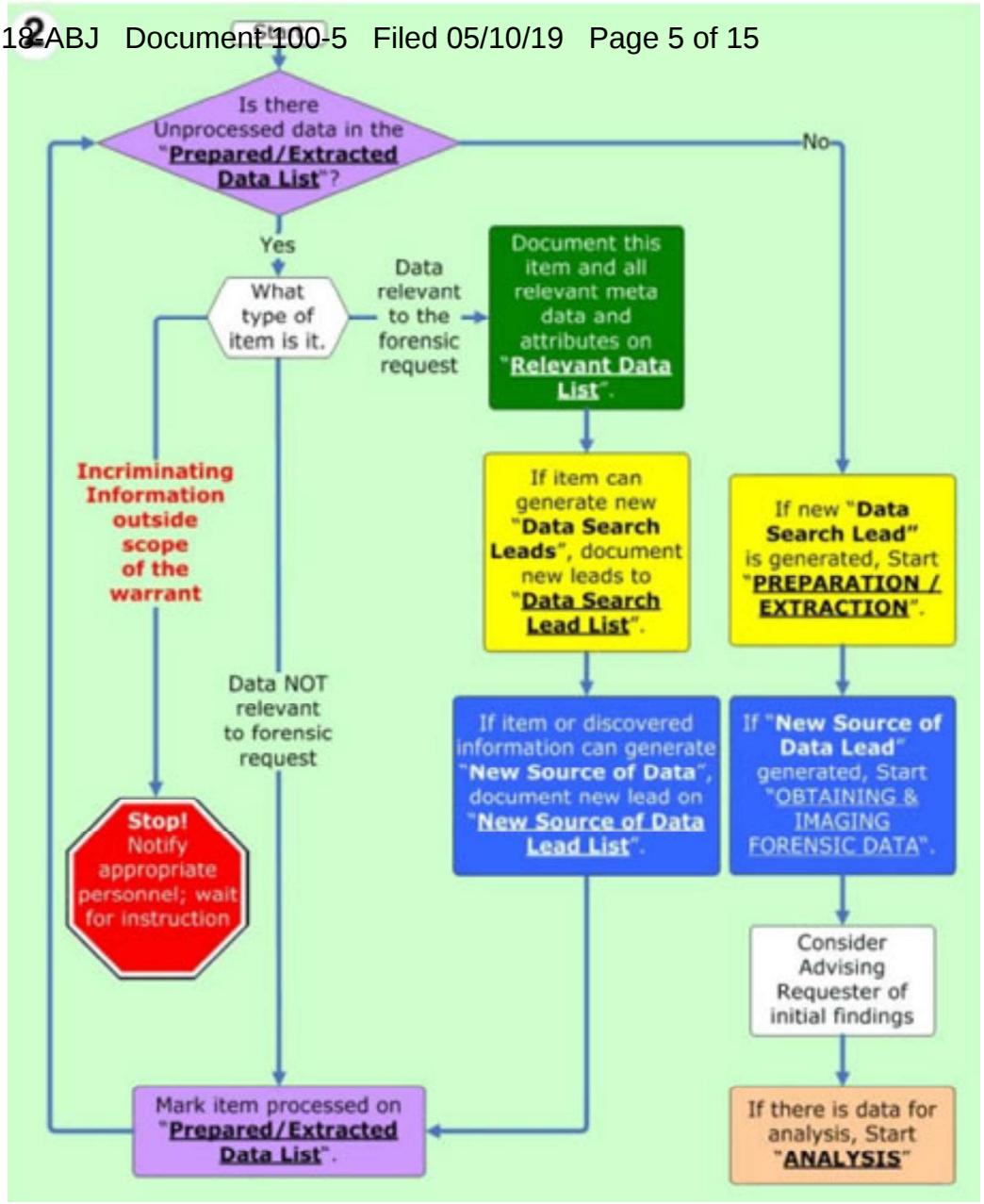


For each search lead, examiners extract relevant data and mark that search lead as processed. They add anything extracted to a second list called an "Extracted Data List." Examiners pursue all the search leads, adding results to this second list. Then they move to the next phase of the methodology, identification.

Identification

Examiners repeat the process of identification for each item on the Extracted Data List. First, they determine what type of item it is. If it is not relevant to the forensic request, they simply mark it as processed and move on. Just as in a physical search, if an examiner comes across an item that is incriminating, but outside the scope of the original search warrant, it is recommended that the examiner immediately stop all activity, notify the appropriate individuals, including the requester, and wait for further instructions. For example, law enforcement might seize a computer for evidence of tax

fraud, but the examiner may find an image of child pornography. The most prudent approach, after finding evidence outside the scope of a warrant, is to stop the search and seek to expand the warrant's authority or to obtain a second warrant.



If an item is relevant to the forensic request, examiners document it on a third list, the Relevant Data List. This list is a collection of data relevant to answering the original forensic request. For example, in an identity theft case, relevant data might include social security numbers, images of false identification, or e-mails discussing identity theft, among other things. It is also possible for an item to generate yet another search lead. An email may reveal that a target was using another nickname. That would lead to a new keyword search for the new nickname. The examiners would go back and add that lead to the Search Lead List so that they would remember to investigate it completely.

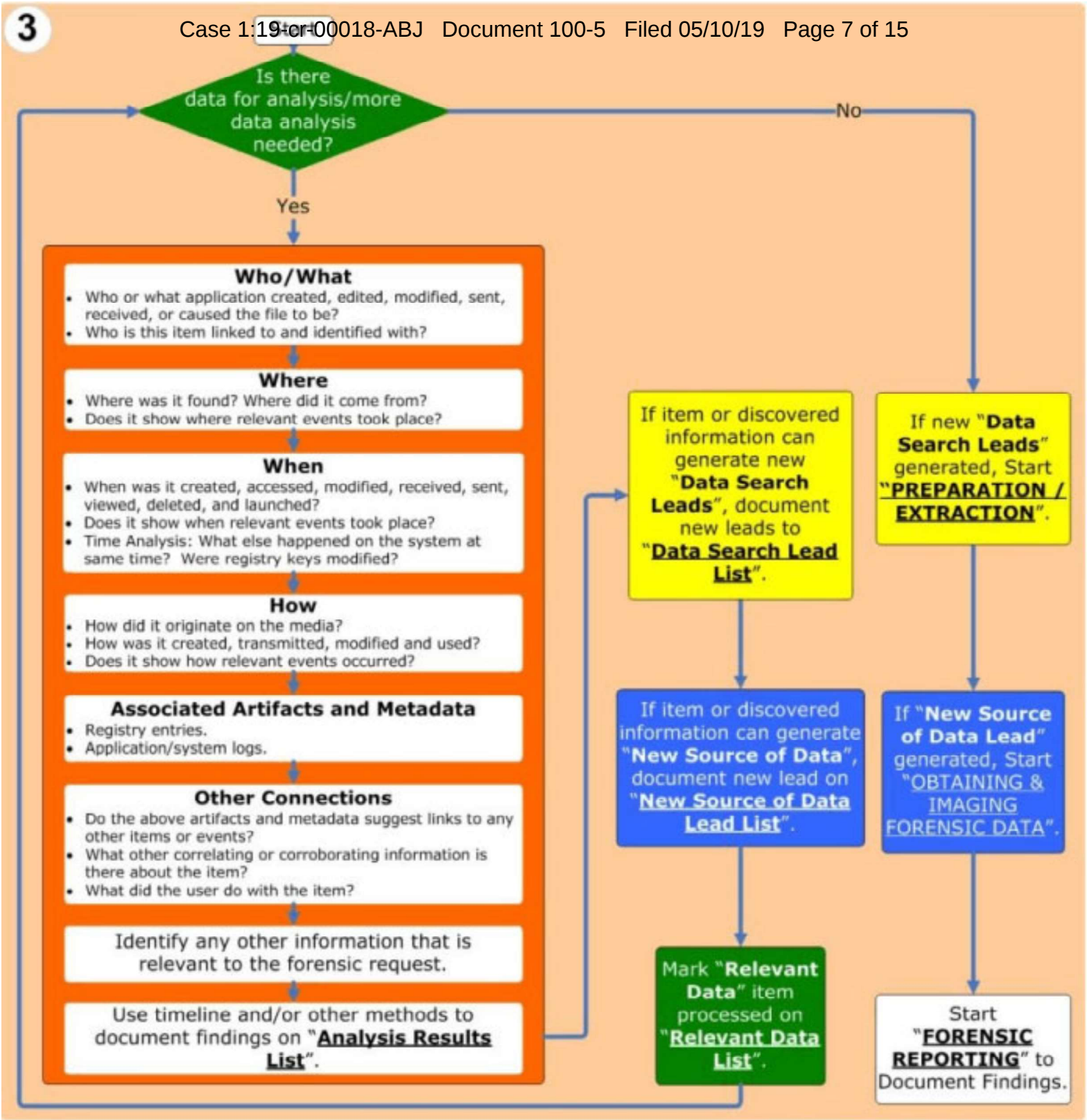
An item can also point to a completely new potential source of data. For example, examiners might find a new e-mail account the target was using. After this discovery, law enforcement may want to subpoena the contents of the new e-mail account. Examiners might also find evidence indicating the target stored files on a removable universal serial bus (USB) drive—one that law enforcement did not find in the original search. Under these circumstances, law enforcement may consider getting a new search warrant to look for the USB drive. A forensic examination can point to many different types of new evidence. Some other examples include firewall logs, building access logs, and building video security footage. Examiners document these on a fourth list, the New Source of Data list.

After processing the Extracted Data list, examiners go back to any new leads developed. For any new data search leads, examiners consider going back to the Extraction step to process them. Similarly, for any new source of data that might lead to new evidence, examiners consider going all the way back to the process of obtaining and imaging that new forensic data.

At this point in the process, it is advisable for examiners to inform the requester of their initial findings. It is also a good time for examiners and the requester to discuss what they believe the return on investment will be for pursuing new leads. Depending on the stage of a case, extracted and identified relevant data may give the requester enough information to move the case forward, and examiners may not need to do further work. For example, in a child pornography case, if an examiner recovers an overwhelming number of child pornography images organized in usercreated directories, a prosecutor may be able to secure a guilty plea without any further forensic analysis. If simple extracted and identified data is not sufficient, then examiners move to the next step, analysis.

Analysis

In the analysis phase, examiners connect all the dots and paint a complete picture for the requester. For every item on the Relevant Data List, examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. Examiners also explain where they found it. Most importantly, they explain why all this information is significant and what it means to the case.



Often examiners can produce the most valuable analysis by looking at when things happened and producing a timeline that tells a coherent story. For each relevant item, examiners try to explain when it was created, accessed, modified, received, sent, viewed, deleted, and launched. They observe and explain a sequence of events and note which events happened at the same time.

Examiners document all their analysis and other information relevant to the forensic request, and add it all to a fifth and final list, the "Analysis Results List." This is a list of all the meaningful data that answers who, what, when, where, how, and other questions. The information on this list satisfies the forensic request. Even at this late stage of the process, something might generate new data search leads or a source of data leads. If this happens, examiners add them to the appropriate lists and consider going back to examine them fully.

Finally, after examiners cycle through these steps enough times, they can respond to the forensic request. They move to the Forensic Reporting phase. This is the step where examiners document findings so that the requester can understand them and use them in the case. Forensic reporting is outside the scope of this article, but its importance can not be overemphasized. The final report is the best way for examiners to communicate findings to the requester. Forensic reporting is important because the entire forensic process is only worth as much as the information examiners convey to the requester. After the reporting, the requester does case-level analysis where he or she (possibly with examiners) interprets the findings in the context of the whole case.

Conclusion

As examiners and requesters go through this process, they need to think about return on investment. During an examination, the steps of the process may be repeated several times. Everyone involved in the case must determine when to stop. Once the evidence obtained is sufficient for prosecution, the value of additional identification and analysis diminishes.

It is hoped that this article is a helpful introduction to computer forensics and the digital forensics methodology. This article and flowchart may serve as useful tools to guide discussions among examiners and personnel making forensic requests. The Cybercrime Lab in the Computer Crime and Intellectual Property Section (CCIPS) is always available for consultation. CCIPS personnel are also available to assist with issues or questions raised in this article and other related subjects.

About the Authors

Ovie L. Carroll is the Director of the Cybercrime Lab in the CCIPS. He has over twenty years of law enforcement experience. He previously served as the Special Agent in Charge of the Technical Crimes Unit at the Postal Inspector General's Office and as a Special Agent with the Air Force Office

of Special Investigations.

Stephen K. Brannon is a Cybercrime Analyst in the CCIPS's Cybercrime Lab. He has worked at the Criminal Division in the Department of Justice and in information security at the Criminal Division in the Department of Justice and in information security at the FBI.

Thomas Song is a Senior Cybercrime Analyst in the CCIPS's Cybercrime Lab. He has over fifteen years in the computer crime and computer security profession. He specializes in computer forensics, computer intrusions, and computer security. He previously served as a Senior Computer Crime Investigator with the Technical Crimes Unit of the Postal Inspector General's Office.

The Cybercrime Lab is a group of technologists in the CCIPS in Washington, DC. The lab serves CCIPS attorneys, Computer Hacking and Intellectual Property (CHIP) units in the U.S. Attorneys' offices, and Assistant U.S. Attorneys, by providing technical and investigative consultations, assisting with computer forensic analysis, teaching, and conducting technical research in support of Department of Justice initiatives.

The Crime Scene Investigator Network gratefully acknowledges the United States Department of Justice, Executive Office for United States Attorneys for allowing us to reproduce the article *Computer Forensics: Digital Forensic Analysis Methodology*.

Cite as: ***56 U S Attorneys' Bulletin, Jan 2008 (https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf)***

Article posted September 12, 2017

Follow the Crime Scene Investigator Network

(http://www.facebook.com/pages/Crime-Scene-Investigator-Network/78490228882)

(http://twitter.com/intent/follow?source=followbutton&variant=1.0&screen_name=CSInetwork)

(http://www.youtube.com/user/csinetwork?sub_confirmation=1)

Receive our Free Newsletter
Receive Job Posting Alerts

Your Email

you@domain.com

☑ **Newsletter (Monthly)**

☐ **Job Postings (Daily)**

Sign up now to receive our free monthly newsletter featuring articles, news and new jobs available in Crime Scene Investigations and Forensic Science.

Privacy Statement
More about the newsletter

Submit

Receive our Free Newsletter
Receive Job Posting Alerts

Your Email

you@domain.com

☑ **Newsletter (Monthly)**

☐ **Job Postings (Daily)**

Sign up now to receive our free monthly newsletter featuring articles, news and new jobs available in Crime Scene Investigations and Forensic Science.

Privacy Statement
More about the newsletter

Submit

(https://www.crime-scene-investigator.net/becomeone.html)

(https://www.crime-scene-investigator.net/csi-training.html)

(https://crime-scene-resources.myshopify.com/collections/frontpage)

(https://crime-scene-resources.myshopify.com/collections/frontpage)

Home (https://www.crime-scene-investigator.net/index.html)
Crime Scene Response (https://www.crime-scene-investigator.net/csi-response.html)
Evidence Collection (https://www.crime-scene-investigator.net/csi-collection.html)
Crime Scene and Evidence Photography (https://www.crime-scene-investigator.net/csi-photo.html)
Articles (https://www.crime-scene-investigator.net/csi-articles.html)
Videos (https://www.crime-scene-investigator.net/csi-video.html)
College and University Programs (https://www.crime-scene-investigator.net/csi-training.html)
Become a CSI (https://www.crime-scene-investigator.net/becomeone.html)
Employment (https://www.crime-scene-investigator.net/employment.html)
Forum (https://www.crime-scene-investigator.net/forum.html)
Resources and Links (https://www.crime-scene-investigator.net/csi-resources.html)
Contact (https://www.crime-scene-investigator.net/contact.html)
Privacy (https://www.crime-scene-investigator.net/privacypolicy.html)
Site Map (https://www.crime-scene-investigator.net/sitemap.html)
Advertise With Us (https://www.crime-scene-investigator.net/advertising.html)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Case No.: 1:19-CR-00018-ABJ

UNITED STATES OF AMERICA,

Plaintiff,

v.

ROGER J. STONE, JR.,

Defendant.
_____/

ORDER

Before the Court is Roger J. Stone's Motion to Suppress. The Court, having considered the Defendant's motion and otherwise being fully advised, finds that the Defendant is entitled to an evidentiary hearing, pursuant to *Franks v. Delaware*, 438 U.S. 154, 156, 98 S.Ct. 2674, 2676 (1978).

It is therefore ORDERED AND ADJUGED that there shall be a *Franks* evidentiary hearing on June 21, 2019.

DONE AND ORDERED in Washington, DC, this_____day of_____, 2019.

_____
AMY BERMAN JACKSON
United States District Judge

cc: all counsel of record