Digital Forensics Evidence Report - CONFIDENTIAL

Final Evidence Analysis Report - Case #77014

Prepared By: Drew Brown

Report Published Date: June 27, 2021

Old Dominion University
CYSE407 Digital Forensics

1.1 DIGITAL FORENSICS EXAMINATION REPORT

Case #77014

INVESTIGATOR:	Bryan Bechard
	Lead NCIS Investigator – Badge #22045
	Norfolk, VA
DIGITAL FORENSICS TECHNICIAN:	Drew Brown
	Forensics Examiner - Badge #277
	Norfolk, VA

SUBJECT:	DIGITAL FORENSICS EVIDENCE REPORT
Accused:	Lieutenant Colonel Davis M. Bernard United States Army
Organization:	North Atlantic Treaty Organization Naval Support Activity Norfolk Office
Offence:	Suspected involvement with Russian state threat actors
Date of Request:	May 15, 2021
Date of Conclusion:	June 27, 2021
Report Published Date:	June 27, 2021

2.1 TABLE OF CONTENTS

3.1 ABSTRACT

This digital forensics report was prepared to communicate the digital forensics processes, findings, and recommendations from evidence pertinent to the ongoing investigation into Lt. Col. Davis M. Bernard's interactions with Russian foreign national operatives. The evidence findings have been appropriately assigned to CASE #77014. Two devices in the possession of Lt. Col. Bernard are a personal cellular device and a laptop. These devices have been forensically processed in a manner that is consistent with Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Archiving Digital and Multimedia Evidence. National Institute of Justice (NIJ) is regularly referenced to ensure up-to-date compliance with the evolving digital forensic processing procedures.

This report intends to aid court officials in making their judgments within the confines of applicable law. Lt. Col. Davis M. Bernard and his chosen legal counsel team have received copies of this digital forensics report.

3.2 CASE BACKGROUND

On Saturday, 15 May 2021, an anonymous tip was received through the FBI crime portal. The tip accuses Lt. Col. Davis M. Bernard to be in "close and continuing" contact with known Russian foreign national operatives. The extent and purposes of the accused interactions remain to be unclear outside of the anonymous tip received.

3.3 SUSPECT SUMMARY

Lt. Col. Davis M. Bernard (US Army) has been assigned to the North Atlantic Treaty Organization offices located at Naval Surface Activity in Norfolk, Virginia since 2017. Since his assigned NATO activity, Lt. Col. Bernard has traveled extensively throughout Eastern Europe and the various territories neighboring the Eastern European region. Lt. Col. Bernard has 23 years of service with the United States Army and has maintained a TS/SCI clearance for the same duration. This individual has access to information which is considered to cause exceptionally grave danger to the United States and its invested interests should the privileged information be exposed to non-privileged persons.

4.1 GENERAL PROCEDURES

1. Consider the preservation of traditional forensic evidence (i.e., fingerprint, DNA)
2. Maintain original media.
3. Create image copies of original media on new or forensically sterile media.
4. Use write blocker during data acquisitions.
5. Verify bit-by-bit image copies.
6. Analyze collected data and establish evidence report.
7. Maintain evidence chain of custody as necessary to maintain audit logs.

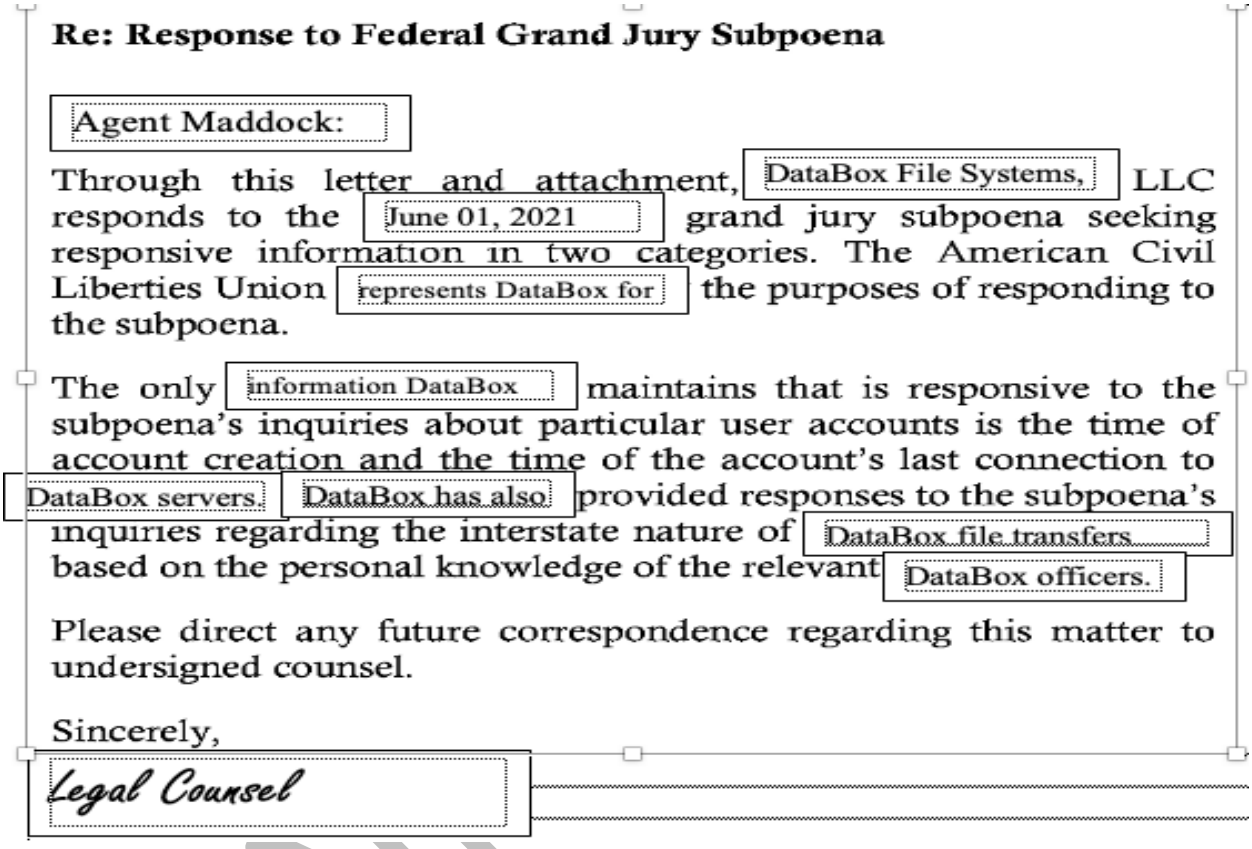
4.2 SEARCH AND SEIZURE

Investigators applied for search warrants and upon approval, seized all evidence believed to be connected to the on-going investigation of close and continued contact with Russian operatives with the accused, Lt. Col. Davis Bernard.

Lt. Col. Bernard is presently represented by a team of legal counselors who deny their clients accused involvement with the alleged transfer of classified materials via online data transfer platform, DataBox. DataBox has been issued subpoenas for server logs relating to any activity carried out by Lt. Col. Bernard via the device IDs contained within this report.

4.2.1 DataBox Subpoena

DataBox File Systems LLC has responded via ACLU representation outlining the information maintained on their servers relating to the subjects of CASE #77014. DataBox is an encrypted file sharing provider.



Re: Response to Federal Grand Jury Subpoena

Agent Maddock:

Through this letter and attachment, DataBox File Systems, LLC responds to the June 01, 2021 grand jury subpoena seeking responsive information in two categories. The American Civil Liberties Union represents DataBox for the purposes of responding to the subpoena.

The only information DataBox maintains that is responsive to the subpoena's inquiries about particular user accounts is the time of account creation and the time of the account's last connection to DataBox servers. DataBox has also provided responses to the subpoena's inquiries regarding the interstate nature of DataBox file transfers based on the personal knowledge of the relevant DataBox officers.

Please direct any future correspondence regarding this matter to undersigned counsel.

Sincerely,

Legal Counsel

4.3 METHODS OF EXAMINATION

4.3.1 Location of Examination

Evidence examination was processed at the regionally accredited Computer Forensics Laboratory maintained by Naval Surface Activity Norfolk.

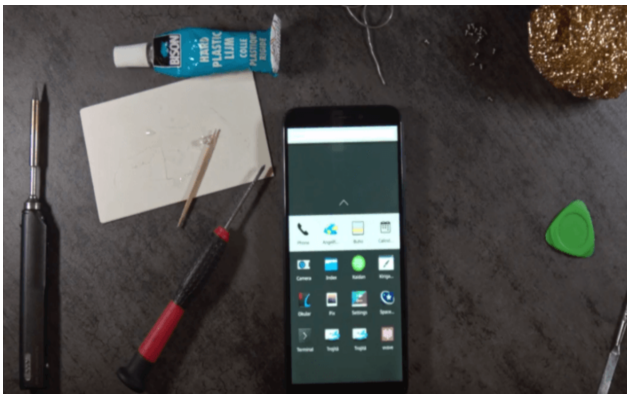
4.3.2 Documentation, Reporting, and Collection Assurances

Court officials can be assured that evidence has been processed and logged according to the NIJ publication (https://www.ncjrs.gov/pdffiles1/nij/199408.pdf) and Scientific Working Group Digital Evidence recommendations as outlined in their Best Practices for Digital Evidence Collection publication (https://drive.google.com/open?id=1zP4OgpRrj-t9sVGNcqndqIgsemq7u5XQ)

5.1 EVIDENCE ITEMS

Evidence artifacts obtained after search warrants executed on Lt. Col. Bernard.

5.1.1 Personal Cellular Device – Linux PinePhone64



S/N: DFD91QZ77001455

OS: PostMarketOS

Specifications:

Quad-Core Allwinner A64 1.152 GHz

3GB LPDDR3 RAM / 32GB eMMC

Quectel EG-25G with worldwide bands

5.1.2 Personal Laptop Device - Lenovo ThinkPad SL510

S/N: 78-12137

OS: Windows 7 Professional (32-bit)

Specifications:

2.53-GHz Intel Core 2 Duo P8700

2GB DDR3 RAM

320GB HDD

5.2 EXTRACTED EVIDENCE

The subcategories on the following page outline the evidence artifacts collected from analyzing the evidence items from section 5.1. EnCase mobile investigator software was used to recover text messages on the personal cellular device. EnCase Forensic software was used to recover email exchanges and deleted zip files which were found to have been uploaded to DataBox.

5.2.1 EnCase Mobile Investigator - Personal Cellular Device – Linux PinePhone64

1. Text exchanges originating from the accused's personal device to a contact labeled "Red Ralph" confirm a lunch meeting took place 2/15/2021.

5.2.2 EnCase Forensic Collection - Personal Laptop Device - Lenovo ThinkPad SL510

1. Logical extraction techniques were used to image the original hard drive of the Lenovo ThinkPad SL510. Analysis procedures recovered deleted zip files of classified materials. The recovered zip file hashings matched web log zip file hashings which concludes classified materials were posted to DataBox via this machine.
2. Email communications between Lt. Col. Bernard and an email address RedRalph@gmail.com revealed several meetings and money transfers for "consulting services"

6.1 CONCLUSIONS AND RECOMMENDATIONS

The analysis of the evidence items provided for CASE #77014 have undoubtedly shown negligent transfer of classified materials from the devices that were in Lieutenant Colonel Davis M. Bernard's possession.

In an effort to contain the exceptionally grave danger Lieutenant Colonel Davis M. Bernard has brought onto the United States, it is my professional recommendation that he be revoked of his TS/SCI credentials immediately. Further investigations are necessary to identify the full extent of classified information that has been stolen and compromised and to ID the Russian foreign national operative contact(s) that Lt. Col. Bernard has voluntarily chosen to identify with.