**Note:**  
  
Data contained in these findings may be sensitive, confidential, or in some cases offensive. It is intended for viewing only by those involved in the investigation, prosecution, defense, and adjudication of this case. Any other viewing is not authorized.  
  
**Executive Summary**  
  
Special Agent Frank Wilson #345 of the Ministry of Wacky Walks, Bureau of Criminal Investigations, requested an examination of evidence for any information regarding the tax investigation in the Al CAPONE case. Special Agent Frank Wilson #345 of the Ministry of Wacky Walks, Bureau of Criminal Investigations, requested an examination of evidence for any information regarding the tax investigation in the Al CAPONE case. On 1931-01-05 Digital Forensic Examiner (DFE) DFE HOLMES attended the warrant at 7244 Prairie Avenue, Chicago Illinois. DFE HOLMES read a copy of the search warrant authorizing the digital forensic analysis of digital computers, DVR’s, phones, cars and media.  
  
**Search Warrant Operation**   
  
**On Scene Triage**   
  
On 1931-01-05, at around 0940 hrs, law enforcement personnel contacted DFE HOLMES stating the location was secured and they were ready for forensic assistance. The entry log was signed upon entry.   
  
A computer was on and running at the front room area of the home. The date and time displayed on the monitor was consistent with the current date and time. DFE HOLMES entered a small office behind the front room. A Night Owl Digital Video Recording (DVR) system appeared on, but the display monitor was not showing any of the camera activity. Later, this DVR was labeled as evidence Item 9. A successful attempt to log into the DVR system with a username of “dvr” and a password of “dvr”, provided by Special Investigator Frank WILSON. The date and time of the DVR system was unable to be verified.   
  
At around 1349 hrs, a forensic storage drive was plugged into a Compaq computer located under the table at the West end of the table. This computer was labeled as evidence Item 15. Belkasoft RAM Capture (no version information available) forensic software was used to copy the random access memory (RAM) of the computer. At around 1403 hrs, the collection finished and the forensic storage drive was removed.   
  
An LGE LM-V600 phone was located in the office. The date and time displayed on the phone was consistent with the current date and time. At around 1420 hrs, the phone was put into airplane mode. This phone was labeled as evidence Item 13.   
  
Magnet Forensics Encrypted Disk Detector (version 3.1.0) forensic software was used to check Item 15 for encryption. The search results did not detect any encryption software. The power cable was removed from the back of the computer to disconnect it from the power source and prepare it for evidence collection.   
  
Property Inventory and Chain of Custody forms were completed for the seized items. DFE HOLMES transported the seized items to the Chicago Investigations Division Evidence Room, located at 569 North Fifth Street, Chicago, IL. The items were placed into Evidence Intake for secure storage.  
  
  
**Forensic Imaging**  
  
**Item 9**  
  
A Night Owl DVR-THD80B-82-HIK DVR (S/N: 858A216153238) was received on 1931-08-02. DFE HOLMES used Tableau Imager 20.3.0, utilizing a Tableau T356789iu write blocker, to conduct a disk to file manual analysis on the Kingston 2383 (S/N: 1234567889.0) 6 TB SATA drive. The image was processed with DVR Examiner. The forensic image hash value was verified prior to processing therby confirming the data remained unaltered prior to processing. "dvr" with a password of "dvr" was a login to this DVR.  
  
Video clips range from 1931-05-22 at 02:03 to 1931-07-28 at 01:00. Channel 1 shows the kitchen. Channel 2 is behind the bar. Channel 3 is in the kitchen sink area. Channel 4 is over the front table. Channel 5, 6, 7 and 8 have no signal. Screenshots of each working camera were taken. If additional image or video or captures are needed they can be acquired up until we return the DVR. Relevant files were exported.

**Item 12**  
  
A 1931 Buick Encore (Carrier: AT&T) vehicle (IMEI: 861536030696002.0) (S/N: 1RBCJASB1ABE05631) (OS: OnStar Gen10) was received on 1931-08-02. On 08/01/31 at 08:49 AM, DFE HOLMES used Berla iVe 3.5.0.29841 to conduct a disk to file forensic extraction.  
The image (MD5 Hash: 1969d0234829205b1682196ba818f7a872b1) was saved as . The imaging process completed with no errors and was verified. The acquisition and verification hash values matched and are listed below:  
  
 Source MD5 hash: 1969d0234829205b1682196ba818f7a872b1  
 Verification MD5 hash: 1969d0234829205b1682196ba818f7a872b1  
  
 The image was processed with Cellebrite Physical Analyzer 8.1.0.7. The forensic image hash value was verified prior to processing therby confirming the data remained unaltered prior to processing.  
  
The registration located in the glove box of this car had ‘Al COPONE’ listed as the registered owner. Apple Car play was synced to to sync up with 13125551212. Relevant files were exported. This vehicle was returned to the owner on 1931-10-02.

**Item 13**  
  
A LGE LM-V600 Verizon phone (MSISDN: 13125551212.0) (IMEI: 3525712230469390.0) (S/N: DNPVABEZJCL9) (OS: Android 11) (Hostname: Als phone) was received on 1931-08-02. On 08/02/1931 at 14:06:48 (-5), DFE HOLMES used Cellebrite UFED 7.56.0.282 to conduct an advanced logical phone extraction..  
The image (MD5 Hash: ad0234829205b9033196ba818f7a872b) was saved as EvidenceCollection.ufdx. The forensic imaging process was completed successfully and verified with no errors. The source hash was calculated and confirmed unchanged before processing. The acquisition and verification hash values matched, ensuring data integrity.  
  
 Source MD5 hash: ad0234829205b9033196ba818f7a872b  
 Verification MD5 hash: ad0234829205b9033196ba818f7a872b  
  
 The image was processed with Cellebrite Physical Analyzer 8.1.0.7 and further analyzed with mac\_apt.exe. The forensic image hash value was verified prior to processing therby confirming the data remained unaltered prior to processing. "AlCOPONE@gmail.com" with a password of "Password1234" was an email configured on this phone.  
  
Al CAPONE gave Frank Wilson 193104 as the pincode to the phone. "AlCAPONE@gmail.com" with a password of "193104" was an email configured on this phone. This phone contained 176 MMS (multimedia messaging service) messages between AlCAPONE@gmail.com and 16185551211 (James). There were message between AlCOPONE@gmail.com and accountant1492@gmail.com. Relevant files were exported. This phone was returned to the owner on 1931-10-02.

**Item 14**  
  
An eckotec (blue) USB storage drive (S/N: 1234) (Hostname: books2) was received on 1931-08-02. DFE HOLMES did not conduct a manual analysis.  
  
This was an empty USB drive. A search for relevant files was conducted and no files were found. This storage drive was returned to the owner on 1931-10-02.

**Item 15**  
  
A Compaq Presario II server (S/N: ABESL65848Z411234) (OS: Window 10) (Hostname: notCompaq) was received on 1931-08-02. On 08/03/31 at 08:49 AM, DFE HOLMES used Tableau Imager 20.3.0, utilizing a Tableau T356789iu write blocker, to conduct a disk to file forensic extraction on the Kingston 2383 (S/N: 1234567889.0) 123 GB SATA drive. A write blocker is a tool that prevents any write access to a device, thus only allowing for read-only access to maintain the integrity of the evidence. The image (MD5 Hash: 6f1ed002ab5595859014ebf0951522d9) was saved as Ex10.e01. The imaging process completed with no errors and was verified. The acquisition and verification hash values matched and are listed below:  
  
 Source MD5 hash: 6f1ed002ab5595859014ebf0951522d9  
 Verification MD5 hash: 6f1ed002ab5595859014ebf0951522d9  
  
 The image was processed with FTK 7.5.1.127 and further analyzed with Arsenal Image Mounter 3.9.223, memdump, magnet encrypted disk detection, Kape. The forensic image hash value was verified prior to processing therby confirming the data remained unaltered prior to processing. "administrator" with a password of "password1234" was a login to this server. "AlCOPONE@gmail.com" with a password of "Password1234" was an email configured on this server.  
  
Quicken and Turbo Tax were both installed on this server. Relevant files were exported. This server was returned to the owner on 1931-10-02.

**Item 69**  
  
A storage drive (Hostname: books1) was received on 1931-08-02. DFE HOLMES conducted a manual analysis.

**Report Conclusion**  
  
This document contains findings regarding the analysis of digital evidence that was submitted for forensic examination. The data contained in these findings and data extractions should not be regarded as evidence, but rather findings concerning that evidence. Contact the case officer or prosecutor to obtain the evidentiary data.  
  
It should be noted that not all files were reviewed during this examination. It is incumbent upon the requester to thoroughly review the data and make a determination as to the probative or exculpatory nature of any and all information.  
  
All forensic equipment and software have been functionally tested/validated without errors prior to use. Where possible, before utilizing stand-alone write blockers, firmware was updated to the current version and functionality was verified.  
  
All forensic acquisition, analysis and write-blocking software used for this case is licensed and/or registered to DFE HOLMES and/or the Ministry of Wacky Walks.  
  
This report contains digital examination of the items provided based on the investigative information and tools available to the examiner at the time of the analysis.   
  
A copy of this report will be given to Frank Wilson #345. Additional analysis may be requested after review of the report or as the investigation continues.  
  
All digital images obtained pursuant to this investigation will be maintained on MWW servers for five years past the date of adjudication and/or case discontinuance. Copies of digital images will be made available upon request. All files copied from the images and provided to the case agent for review are identified as the DIGITAL EVIDENCE FILE and will be included as an item in the case file.