



MORRIS COUNTY PROSECUTOR'S OFFICE

Administration & Records Bldg.

P.O. Box 900

Morristown, New Jersey 07963-0900

Robert J. Carroll

Prosecutor

Margaret M. Calderwood

First Assistant Prosecutor

Telephone: 973-285-6200

Fax: 973-285-6226

morriscountynj.gov/prosecutor

ProsecutorOPRA@co.morris.nj.us

Robert M. McNally

Chief of Detectives

January 26, 2024

VIA Email:

Citizen Voice Media

opra+request-56902-04fc259c@requests.opramachine.com

RE: MCPO OPRA File Number 24-0002

Dear Citizen Voice Media:

The Morris County Prosecutor's Office received your Open Public Records Act (OPRA) request dated January 8, 2024, on January 8, 2024, and it was received by the records custodian on the same date. On January 18, 2024, our Office replied to your request, therein, indicating that an extension to Friday, January 26, 2024, was necessary to continue our search and review of our policies and procedures and other records which might be responsive to your request. You requested the following:

1. Accreditation certifications for any digital media, phone, or technology/digital forensics labs in the sheriff's office, county police, or prosecutor's office.
2. All policies and procedures for handling digital evidence and conducting examination for any county digital forensics lab.
3. List of all digital forensics softwares and hardwares in use by any county entity for law enforcement purposes.
4. What accreditation bodies have a accredited or certified any county digital forensics lab or unit?

Regarding Item #1 of your request, our Office does not possess any responsive records. As for your inquiry concerning records from the Sheriff's Office, the Office of the Morris County Prosecutor would not possess any records responsive to your request. Please contact the following agency with your inquiry:

- Morris County Sheriff's Office:
 - <https://www.morriscountynj.gov/Departments/Sheriff/About-Us/Sheriff-Open-Public-Records-Act-OPRA-Requests>
 - Please note that Morris County does not have a County Police department.

Regarding Item #2 of your request, the following records are being provided and are responsive to your request:

1. Morris County Prosecutor's Office HTCUC Directive (5 pages).
2. Morris County Prosecutor's Office HTCUC SOP (12 pages).

Note: *Redactions have been made to the above supplied records where they may reveal "surveillance, security, tactical, investigative, or operational techniques, measures, or procedures, which, if disclosed, would create a risk to the safety of persons" and "compromise [our] agency's ability to effectively conduct investigations." See N.J.S.A. 47:1A-6 and N.J.A.C. 13:1E-3.2(a)2. See also Naeem Akhtar v. NJ Department of Law & Public Safety, Division of Criminal Justice Custodian of Record, GRC Complaint No. 2014-344 (September 29, 2016) and Cattoner v. Township of Jackson Police Department (Ocean) Custodian of Record, GRC Complaint No. 2011-230 (December 18, 2002). OPRA does not abrogate an exemption of a public record pursuant to any other statute. N.J.S.A. 47:1A-9(a).*

Regarding Item #3 of your request, said request is "invalid under OPRA because it fails to specifically name identifiable government records and because the request requires research beyond the scope of a custodian's duties pursuant to MAG Entm't, LLC v. Div. of ABC, 375 N.J. Super. 534, 546 (App. Div. 2005); Bent v. Twp. of Stafford Police Dep't, 381 N.J. Super. 30, 37, (App. Div. 2005); N.J. Builders Ass'n v. N.J. Council on Affordable Hous., 390 N.J. Super. 166, 180 (App. Div. 2007); Feiler-Jampel v. Somerset Cnty. Prosecutor's Office, GRC Complaint No. 2007-190 (Interim Order dated March 26, 2008)." Chatfield v. N.J. Dept. of Corrections, GRC Complaint No. 2021-121 (November 2022). OPRA did not countenance "'information to be analyzed, collated and compiled by the responding government entity' or 'open-ended searches of an agency's files' ... 'A records request must be well defined so that the custodian *knows precisely what records are sought*. The request should not require the records custodian to undertake a subjective analysis to understand the nature of the request.'" Paff v. Galloway Township, 229 N.J. 340, 355 (2017) (citations omitted) (emphasis supplied).

Instructive guidance has been provided by the Appellate Division when it concluded that "while an exact definition of an impermissibly overly broad request is abstract, courts have found requests that require a custodian to exercise his discretion, survey employees, or undertake research to determine whether a record is responsive are overly broad and not encompassed by OPRA." Shipyard Associates, L.P. v. City of Hoboken, A-3794-13T1, 2015 WL 10352982, at *4 (N.J. Super. Ct. App. Div. Sept. 1, 2015).

Further, the Government Records Council has also decided that a “custodian [is] under no obligation to provide a record that had not been created at the time of an OPRA request.” Goeckel v. Chatham Borough Police Dep’t (Morris), GRC Complaint No. 2013-356 (July 2014) (citing Blau v. Union Cnty., GRC Complaint No. 2003-75 (January 2005)). “OPRA only allows requests for records, not requests for information”; to qualify under OPRA, “the request must reasonably identify a record and *not generally* data, information or statistics.” Bent v. Township of Stafford Police Dep’t, 381 N.J. Super. 30, 37 (App. Div. 2005) (emphasis added).

Additionally, records containing such information would be considered confidential as disclosure may reveal “surveillance, security, tactical, investigative, or operational techniques, measures, or procedures, which, if disclosed, would create a risk to the safety of persons” and “compromise [our] agency’s ability to effectively conduct investigations.” See N.J.S.A. 47:1A-6 and N.J.A.C. 13:1E-3.2(a)2. See also Naeem Akhtar v. NJ Department of Law & Public Safety, Division of Criminal Justice Custodian of Record, GRC Complaint No. 2014-344 (September 29, 2016) and Cattoner v. Township of Jackson Police Department (Ocean) Custodian of Record, GRC Complaint No. 2011-230 (December 18, 2002). OPRA does not abrogate an exemption of a public record pursuant to any other statute. N.J.S.A. 47:1A-9(a).

Regarding Item #4 of your request, our Office does not possess any responsive records.

You have also requested the records under the common law. Access under the common law requires that “the person seeking access must ‘establish an interest in the subject matter of the material’.” Mason v. City of Hoboken, 196 N.J. 51, 67 (2008) (quoting Keddie v. Rutgers, 148 N.J. 36, 50 (1997)). As your request fails to declare a particularized interest in the non-supplied requested records, upon which a balancing of interests may be assessed, access to these records is also denied under common law. See O’Boyle v. Borough of Longport, 218 N.J. 168, 200 (2014).

The Office of the Morris County Prosecutor reserves the right to raise any other grounds for denial not raised in this response. Failure of the Office of the Morris County Prosecutor to assert an exception or privilege does not act as a waiver of any grounds for denial. Furthermore, a reviewing Court or the Government Record’s Council (“GRC”) may deem a denial of access to be authorized on grounds other than those advanced by a custodian. Paff v. Twp. of Plainsboro, A-2122-05T2, 2007 WL 957289, at *2 (N.J. Super. Ct. App. Div. Apr. 2, 2007) aff’g, Paff v. Township of Plainsboro, GRC Complaint No. 2005-29 (March 2006).

You have a right to challenge the decision by the Office of the Morris County Prosecutor to deny access. At your option, you may either institute a proceeding in the Superior Court of New Jersey or file a complaint with the GRC by completing Denial of Access Complaint Form. You may contact the GRC by toll-free telephone at 866-850-0511, by mail at PO Box 819, Trenton, NJ, 08625, e-mail at grc@dca.state.nj.us, or on the GRC’s website at www.state.nj.us/grc. The Council can also answer other questions about the law. All questions regarding complaints filed in Superior Court should be directed to the New Jersey Superior Court Clerk.

Note that any challenge to a denial of a request for records under the common law cannot be made to the GRC, as the GRC only has jurisdiction to adjudicate challenges to denials of OPRA requests. A challenge to the denial of access under the common law can be made by filing an action in

Superior Court. All questions regarding complaints filed in Superior Court should be directed to the New Jersey Superior Court Clerk.

This OPRA request is now considered answered and closed.

Sincerely,

A handwritten signature in blue ink, appearing to be 'TS' with a long horizontal stroke extending to the right.

Thomas C. Schmid
Assistant Prosecutor || Custodian of Records

Knab, Meghan G.

From: Citizen Voice Media <info@citizenvoice.com>
Sent: Monday, January 8, 2024 12:17 PM
To: Prosecutors OPRA Requests
Subject: OPRA request - Mobile forensics labs

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear MCPO,

This is a request for public records made under OPRA and the common law right of access. I am not required to fill out an official form. Please acknowledge receipt of this message.

Records requested:

1. Accreditation certifications for any digital media, phone, or technology/ digital forensics labs in the sheriff's office, county police, or prosecutor's office.
2. All policies and procedures for handling digital evidence and conducting examination for any county digital forensics lab.
3. List of all digital forensics softwares and hardwares in use by any county entity for law enforcement purposes.
4. What accreditation bodies have a accredited or certified any county digital forensics lab or unit?

Yours faithfully,

Citizen Voice Media

RECEIVED
By Meghan Knab at 1:12 pm, Jan 08, 2024

Please deliver records electronically via email to the below UNIQUE address for all replies to this request:
opra+request-56902-04fc259c@requests.opramachine.com

Is ProsecutorOPRA@co.morris.nj.us the wrong address for OPRA requests to Morris County Prosecutor's Office? If so, please contact us using this form:

https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fopramachine.com%2Fchange_request%2Fnew%3Fbody%3Dmcpo&data=05%7C02%7CMKnab%40co.morris.nj.us%7Cb982b1e2c605411f9f0608dc106db16a%7Cec2ce8c138394008b949e2b17cfa906d%7C0%7C0%7C638403310530690344%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6IjEhaWwiLCJXVCi6Mn0%3D%7C41000%7C%7C%7C&sdata=yITdhGEotSwvXuGBc07FXbc3ToW2ZfFM%2B71nbqQCM5w%3D&reserved=0

Disclaimer: This message and any reply that you make will be published on the internet. Our privacy and copyright policies:

<https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fopramachine.com%2Fhelp%2Fofficers&data=05%7C02%7CMKnab%40co.morris.nj.us%7Cb982b1e2c605411f9f0608dc106db16a%7Cec2ce8c138394008b949e2b17cfa906d%7C0%7C0%7C638403310530690344%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6IjEhaWwiLCJXVCi6Mn0%3D%7C41000%7C%7C%7C&sdata=yITdhGEotSwvXuGBc07FXbc3ToW2ZfFM%2B71nbqQCM5w%3D&reserved=0>

il6lk1haWwiLCJXVCI6Mn0%3D%7C41000%7C%7C%7C&sdata=MWrHI4pxx4Nt%2FSv2acB2SMLYUgdri99wBYL6jpRi3Jg%3D&reserved=0

View this OPRA request & responses online:

https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Foprachine.com%2Frequest%2Fmobile_forensics_labs&data=05%7C02%7CMKnab%40co.morris.nj.us%7Cb982b1e2c605411f9f0608dc106db16a%7Cec2ce8c138394008b949e2b17cfa906d%7C0%7C0%7C638403310530690344%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiIl6lk1haWwiLCJXVCI6Mn0%3D%7C41000%7C%7C%7C&sdata=h1ovcRkrqSNPKW3jyMpSzEzJgGL1mQNfm3eTTiGDBel%3D&reserved=0

Please note that in some cases publication of requests and responses will be delayed.

If you find this service useful as an OPRA custodian, please ask your web manager to link to us from your organisation's website.

MORRIS COUNTY PROSECUTOR'S OFFICE DIRECTIVE		
SUBJECT: HIGH TECH CRIMES UNIT	NUMBER: Volume 3 Chapter 28	
EFFECTIVE DATE: May 12, 2021	DISTRIBUTION TO: All Municipal and County Law Enforcement Agencies Operating in Morris County	ISSUED BY: Acting Prosecutor Robert J. Carroll
CANCELLATION DATE:		APPROVED BY: Acting Prosecutor Robert J. Carroll

PURPOSE:

Contemporary criminal investigations and subsequent prosecutions often involve the use of digital evidence, therefore the proper identification, collection, recovery and analysis of such evidence by law enforcement are all critical tasks to be performed. As the design of electronic devices and the associated facilitating technology constantly evolves, so do the methods used to secure digital evidence. To this end, the Morris County Prosecutor's Office High Tech Crimes Unit is available to assist municipal, county, state and federal law enforcement agencies with the recovery and preservation of electronic devices, as well as data extraction of digital evidence.

DIRECTIVE:

All municipal and county law enforcement agencies operating within Morris County are directed to contact the Morris County Prosecutor's Office (MCPO) High Tech Crimes Unit (HTCU) when a criminal investigation involves the recovery or seizure of electronic devices and media, including but not limited to cellular telephones, computers, tablets, mobile devices, computer and digital media (Data Storage Devices) including Hard Drives, Portable Hard Drives, Removable Drives, Flash Memory, USB Drives, as well as DVD's, CD's, Disks and Memory Cards.

METHOD OF CONTACT:

An MCPO High Tech Crimes Unit Duty Detective is on call and available (24) hours a day, (7) days a week. The Duty Detective can be reached during regular business hours by calling the MCPO-HTCU at (973) 285-6300, or through the Morris County Communication Center at (973) 285-2900 after regular business hours. Please ensure that these notification requirements and methods are adhered to by members of your agency.

PROCEDURE:

A. Data Extractions

1. All extractions of cellular telephones, computers, tablets, mobile devices, computer and digital media (Data Storage Devices) including Hard Drives, Portable Hard Drives, Removable Drives, Flash Memory, USB Drives, as well as DVD's, CD's, Disks, Memory Cards, and similar or associated electronic devices shall be conducted by the MCPO-HTCU.
2. All requests for other agencies and/or laboratories and vendors (e.g. The Regional Computer Forensics Laboratory, Federal Agencies, or private corporations) to conduct forensic extractions of such electronic evidence must be pre-approved by the assigned case Assistant Prosecutor and the Chief Assistant Prosecutor of the MCPO Special Operations Division.

B. Evidence Submissions to MCPO High Tech Crimes Unit (HTCU)

1. Upon recovery/seizure of electronic devices, investigating law enforcement personnel shall complete the attached High-Tech Crimes Unit Submission Request form and continuation page(s) if necessary, and submit same via email to MCPOHTCU@co.morris.nj.us with a copy of the legal process (Search Warrant, CDW, Consent) and all associated Investigative/Incident Report(s).
2. All portable electronic devices (cellular phones, tablets, laptops, ex.), should [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Contact the HTCU if assistance is required in preserving evidence prior to submission.
3. The submission form will be reviewed by the assigned HTCU Detective and a determination will be made regarding the compatibility of the device to the current forensic technology.
4. The HTCU Detective will contact the submitting personnel to review the case and items to be examined.
5. If the investigation involves multiple devices, the HTCU Detective and investigating personnel will telephonically discuss the investigation to determine which devices should be prioritized for examination. Note: In cases of multiple devices, (3) devices will be accepted, examined and returned before accepting additional devices for examination, unless otherwise authorized by an HTCU supervisor.
6. Once the case and devices are approved for acceptance by the HTCU, an appointment will be made with the investigating personnel to transfer the evidence to the HTCU facility.

7. When delivered to the HTCUC, all evidence will be logged in by the HTCUC Detective in the presence of the submitting personnel, and a copy of the associated HTCUC Evidence Custody Form provided upon completion.
8. During the course of the examination, the forensic examiner will determine the best method of preserving the electronic evidence and if necessary contact the submitting personnel to discuss preservation/production of data options/media (e.g. disk, thumb drive or external hard drive).
9. Upon completion of the forensic extraction/examination, the submitting personnel will be contacted and an appointment scheduled for retrieval of the evidence. The appointment date shall be within (5) business days of the notification.
10. HTCUC Deviations/Exceptions
 - a. If warranted, for emergent circumstances or specific case needs, an HTCUC Detective will respond to a crime scene or event to recover electronic devices, and/or to accept devices from investigating personnel that require immediate examination/evidence preservation.
 - b. A response and/or case assignment to the MCPO HTCUC will be evaluated on a case-by-case basis for each criteria and device. When applicable, the HTCUC Supervisor will confer with other involved MCPO Unit Supervisor(s) concerning this decision.
 - c. Agencies may also be instructed to submit evidence without an appointment if the matter is emergent. Such submissions to HTCUC will still require a completed High-Tech Crimes Unit Submission Request form at the time of submission/transfer to HTCUC.

		MORRIS COUNTY PROSECUTOR'S OFFICE HIGH TECH CRIMES UNIT – SUBMISSION FORM		<i>Official Use Only</i> HT #	
MCPO Unit (if assigned):		MCPO Case # (if assigned):		Promis Gavel #:	
Case Agency(s) & Case Agency Case #:					
Crime/ Type of Investigation:		N.J.S.:		Crime Date:	Crime Time:
Location of Crime:					
Person Reporting Incident / Crime:					
Suspect(s):		Person Info(s):		Address(s):	
Victim(s):		Person Info(s):		Address(s):	
Stolen / Missing Property:			Weapon Used:		

AGENCY INFORMATION		
Case Detective:	Request Date:	Date Evidence Seized:
Submitting Agency:		Legal Authority to Search: (SW, Consent, Other*)
Submitted by:	Phone / Cell Number:	Email Address:

DEVICES TO BE SUBMITTED				
HTCU Item #:	Description:		Lost Power?	Passcode:
Make:	Model:	Serial #:	Agency Item #:	
HTCU Item #:	Description:		Lost Power?	Passcode:
Make:	Model:	Serial #:	Agency Item #:	
HTCU Item #:	Description:		Lost Power?	Passcode:
Make:	Model:	Serial #:	Agency Item #:	

Miscellaneous Notes (include which items have been previously examined or manually scrolled)

Used Continuation Form: ☐

Include a copy of the Investigation Report as well as a copy of the signed Affidavit/Consent Form. A maximum of three (3) items may be submitted at a time. All submission forms are to be sent to MCPOHTCU@co.morris.nj.us, at which time a member of the High Tech Crimes Unit will contact the submitter after a review of these documents to set up an appointment to submit the items. If there are more than three (3) items, list them on the continuation form and a member of HTCU will telephonically review these devices with the submitter and determine which three (3) will be submitted first.

MORRIS COUNTY PROSECUTOR'S OFFICE STANDARD OPERATING PROCEDURE				
VOLUME:	CHAPTER:	# OF PAGES: 12		
SUBJECT: High Tech Crimes Unit				
EFFECTIVE DATE: January 1, 2006		ACCREDITATION STANDARDS:	REVISION DATE	PAGE #
BY THE ORDER OF: PROSECUTOR FREDRIC M. KNAPP			February 5, 2019	
SUPERSEDES ORDER #:			November 5, 2014	

I. Purpose

The Morris County Prosecutor's Office High Tech Crimes Unit (HTCU) has multiple functions that relate to the use of high-tech devices (computers, cellular phones, tablets, digital cameras, digital audio/video recorders, Global Positioning System (GPS) units, etc., and/or the Internet), either as an instrument of a crime, or to investigate crime. These functions are more specifically identified as follows:

- Forensic Analysis/Computer Crimes/Intrusions
- Technical Services

Each of these functions has a unique role associated with their investigative support, more thoroughly explained below in sections III and IV.

The High Tech Crimes Unit also assists other Units within the Morris County Prosecutor's Office, other law enforcement agencies operating in Morris County, and state and federal law enforcement agencies with these types of investigations.

II. Policies And Procedures

A. Notification And Response

A High Tech Crimes Unit Detective is on call 24 hours a day, 7 days per week, to provide any necessary assistance to any units/personnel in this Office, and to any local, county, state or federal law enforcement agency seeking assistance. All requests for assistance must be reviewed and approved by the unit supervisor.

During normal business hours, contact with the High Tech Crimes Unit can be made by calling (973) 285-6300, and after-hours through the Morris County Communications Center at (973) 285-2900. Non-emergent requests for assistance can be emailed to the High Tech Crimes Unit at hightechcrimes@co.morris.nj.us.

Morris County Prosecutor's Office Detectives and municipal police departments should make every effort to contact a High Tech Crimes Unit detective directly when requesting assistance.

B. Opening Investigation Files

1. All High Tech Crimes Unit members are required to open an investigation file in InfoShare ("X file") **ONLY** when conducting an Original Investigation (OI) of a Computer Crime as defined in N.J.S.A. 2C:20-23, or when the MCPO unit being assisted by the High Tech Crimes Unit does not already have an investigation file ("X file") for said investigation.
2. High Tech Crimes Unit personnel shall open and maintain Original Investigations (OI) files in the standard manner set forth in the Morris County Prosecutor's Office Policy and Procedure Manual, and prepare/submit an initial Investigation Report in the following instances:
 - a. Original or assigned investigations;
 - b. Whenever Issuing a Grand Jury Subpoena;
 - c. Performing any forensic examination for a municipal, county or outside law enforcement agency;
3. If forensic work is requested by another Unit within the Morris Country Prosecutor's Office, all reports will be written under that Unit's case file in InfoShare; the file number ("X number") assigned by the other Unit will be used for all Supplemental Reports.
4. Original Investigations (OI) files opened under the High Tech Crimes Unit, and all reports and events, will be maintained within the High Tech Crimes Unit section

in InfoShare, pursuant to Morris County Prosecutor's Office Policy & Procedure, Volume 3, Chapter 10 (Criminal Case Management).

5. For forensic work being done on an investigation assigned to another Unit in this Office, the detective assigned to the investigation will add the High Tech Crimes Unit Detective to the casefile within InfoShare. The High Tech Crimes Unit Detective will then upload all materials associated with the investigation into InfoShare and transfer custody of physical items to the assigned case detective.
6. All OI files and work files will be tracked on the High Tech Crimes Unit Case Inventory for timely completion.

C. Closing Investigation Files

High-Tech Crimes Unit Original Investigations (OI) files may not always lead to an arrest of a suspect. Occasionally, investigations will be closed out with no further action or turned over to the municipality for further investigation. Any investigation file that does not result in an arrest must be closed out as follows:

1. The case detective shall draft the Internal Disposition Memorandum (IDM) and link it to the InfoShare case management system.
2. The IDM shall include all noteworthy information for a synopsis, factual basis, and reasons for the disposition being requested. All reasonable investigative steps must be conducted prior to closing out an investigation.
3. Prior to drafting the IDM, the case detective shall meet with the Unit Supervisor and Assistant Prosecutor, review the investigation and determine if any further investigative action is necessary to warrant a closeout. A notation on the IDM shall reflect that the Unit Supervisor and Assistant Prosecutor approved the IDM for closeout.
4. If the investigation was a referral from another agency, such as a municipal, state or federal law enforcement agency, or the National Center for Missing and Exploited Children (NCMEC), notification shall be made to that agency, and the New Jersey State Police who track all NCMEC referrals for the State of New Jersey, with a reason for the disposition.

Work files in the High Tech Crimes Unit shall be closed out promptly once all the requested work and accompanying Investigation and Supplemental Reports are completed. The request to close the file must be summarized on the Notes page on the left side of the file and be submitted through the chain of command for review/approval. This is referred to as a "left side file closeout".

D. Issuing a Communications Data Warrant (CDW)

1. Other Unit detectives within the Morris County Prosecutor's Office will prepare their own CDWs. High Tech Crimes Unit Detectives will be available to assist in the technical language and provide certification affidavits when requested.

E. Preparation and Execution of Search Warrants

1. Members of the High Tech Crimes Unit may be called upon to assist in search warrants specifically relating to the collection of electronic evidence, as well as Original Investigations being conducted by Unit members.
2. Prior to the execution of a search warrant, the High Tech Crimes Unit member(s) will prepare all equipment needed to acquire specific electronic evidence that may be found as a result of the search warrant.
3. The Morris County Prosecutor's Office Operations Brief will describe, in detail, the location of the search, search warrant team member assignments and a brief description of the investigation.
4. It is the responsibility of the High Tech Crimes Unit Detective to make it known that computer equipment is not to be handled unless specifically requested by that detective. If a High Tech Crimes Unit Detective will not be attending the actual search, a detective assigned to the search warrant should make contact with the High Tech Crimes Unit Detective for further instructions.
5. A systematic search will be conducted, and all items of evidentiary value will be seized and itemized as evidence. In many circumstances, the Morris County Sheriff's Office Crime Scene Investigations (CSI) will be available to assist with the photography, seizure, and storage of computer equipment. It is acceptable practice to allow MCSO/CSI members to locate, photograph, seize and store computer equipment.
6. If a High Tech Crimes Unit Detective is present during the execution of the search warrant, he/she must fill out a "Computer Seizure Worksheet" for each computer seized. This worksheet is located on the [REDACTED] drive of the office computer network in the "[REDACTED]" folder.
7. If computer equipment is to be seized and retained by a High Tech Crimes Unit Detective, an Inventory Receipt and Return form detailing this equipment must be completed. This Inventory Receipt and Return form may be left at the scene along with a copy of the search warrant, or given to an appropriate individual, according to Morris County Prosecutor's Office guidelines. The original Inventory Receipt and Return form shall be filed with the issuing judge the following business day, or as soon as practical.

F. Consent to Search / Consent to Seize

1. In some circumstances, a detective may request that an individual consent to having their computer / electronic equipment searched. A Morris County Prosecutor's Office "Consent to Search" form must be completed before such a search can proceed.
2. On-Site previews will be in accordance with the Unit member's level of training and experience, and all aspects of an on-site preview will adhere to the High Tech Crimes Unit forensic examination procedures, and will be fully documented.
3. The High Tech Crimes Unit Detective may request an individual to consent to having their computer / electronic equipment seized and searched outside of his/her presence. The individual signing the Consent to Search form must be made aware that they are waiving their right to be present during this search.
4. A victim or witness involved in an investigation may consent to a forensic examination of their electronic equipment.

G. Preservation Letters

1. If required by the individual investigation, the assigned detective shall, as soon as possible, send the appropriate preservation letter to the Internet Service Provider (ISP). These letters should be sent immediately since many ISPs hold information regarding Internet Protocol addressing and E-Mails for a very short period of time before they are purged from their system.
2. Remain cognizant that for most ISPs, the account will no longer be accessible to the account holder once the account is preserved.
3. Remain cognizant that most ISPs will notify the account holder that law enforcement is investigating them. In these instances a nondisclosure order must be applied for by the case detective.

III. Forensic Analysis/Computer Crimes/Intrusions

The High Tech Crimes Unit will have an ongoing demand to conduct computer forensic examinations of seized computers and electronic devices. Forensic examinations will be performed at the request of Morris County Prosecutor's Office Detectives and other local, county, state and federal law enforcement agencies as needed.

The rationale behind the need to conduct forensic examinations is to assist other law enforcement agencies with their investigations and to provide additional leads or proofs contained within the submitted evidence being examined.

The High Tech Crimes Unit is responsible for investigating all Computer Crime violations as defined in N.J.S.A. 2C:20-23.

Additionally, the High Tech Crimes Unit shall investigate all Network Intrusions, technical aspects of Cyber-Stalking, Financial Hacking, Cyber-Terrorism, Cryptocurrency Investigations and various other related high-tech related crimes.

A. Receiving Evidence for Forensic Examination

1. No evidence will be received by the High Tech Crimes Unit without the submission of either a copy of an approved Search Warrant or a signed Consent to Search form. No evidence will be held within the High Tech Crimes Unit while applications are being made for a Search Warrant.
2. If the equipment is seized by an outside agency and the matter is not being jointly investigated with another MCPO Unit, the assigned High Tech Crimes Unit Detective will be required to open a case file in InfoShare.
3. All individuals submitting seized equipment must first complete the "[REDACTED]" located on the "[REDACTED]" drive of the office computer network in the "[REDACTED]" folder.
4. The case detective or other law enforcement officer having knowledge of the case must complete the "[REDACTED]" with specific details of the case, e-mail addresses / screen names of individuals, and keywords / phrases to be searched before an examination can begin. If these forms are not completed, or the equipment submitted does not coincide with the evidence on the inventory receipt, the evidence will not be examined by the High Tech Crimes Unit. It will be the responsibility of the intake detective to insure that the Request Form is completed and contains the necessary information.
5. All incoming evidence will be properly labeled, using a "[REDACTED]" located on the "[REDACTED]" drive of the office computer network in the "[REDACTED]" folder.
6. A case folder will be completed for all evidence being submitted for examination unless a case folder had been previously generated.
7. The following steps will be followed when receiving evidence:
 - a. The submitting law enforcement personnel will complete the "[REDACTED]" and will provide copies of police reports, investigation reports and supplemental reports.

- b. Open case folder (as noted above under II. B.), complete it and insert all of the provided reports. Ensure that a MCPO "X Number" is assigned for the case examination. Only one "X Number" should be assigned per case.
 - c. Ensure that the computer / electronic evidence items are stored in a secure, locked area. If the Morris County Prosecutor's Office Evidence Room is unavailable, the High Tech Crimes Unit Office is a suitable temporary location.
8. Shipping of evidence to private labs or law enforcement agencies for lab assistance (i.e. [REDACTED]), shall be done as follows:
- a. All evidence must be shipped using the Morris County Prosecutor's Office FedEx Account, using Priority Service with a signature confirmation as a mandatory protocol.
 - b. The case detective must track the package using FedEx and upon receipt, print out all of the shipping & tracking information from FedEx.com.
 - c. A follow up email/telephone call by the case detective to the receiving lab/agency will follow as soon as possible.
 - d. Direct communications with the receiving lab/agency for confirmation when the lab work is completed and when the evidence has been shipped for return to MCPO.
 - e. The case detective will track the return FedEx package from the lab/agency and when received by the Morris County Mail Room, and will print out all tracking information.
 - f. The case detective must pick up said evidence from the Morris County Mail Room.
 - g. Upon receipt of the evidence back to the HTCUC, the case detective will maintain all shipping copies in the case file and provide same to the requesting MCPO unit for their case file.
 - h. Upon receipt of the evidence back to the HTCUC, the case detective will proceed with the forensic examination as per standard practice.
 - i. The shipping, tracking and receipt of the evidence at the lab and return shipping receipt to MCPO HTCUC will all be documented in the final examination report of said evidence.

B. Computer Forensic Examination Guidelines (All Electronic Evidence)

The following are general guidelines for conducting a forensic examination on evidence submitted:

1. **All attempts to [REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED] (Owner, Case Detective, Assistant Prosecutor, Etc.)
2. All procedures and methods completed will be recorded on the [REDACTED] located on the [REDACTED] drive of the office computer network in the "[REDACTED]" folder. This worksheet is discoverable, should you be required to testify to your course of action in court.
3. Only use software registered to either the forensic examiner, the Morris County Prosecutor's Office, or any other law enforcement agency for the examination. It is acceptable to use "shareware" that offers an evaluation period during the course of the examination, as long as the software and methods used are recorded within the "[REDACTED]".
4. When required, using a [REDACTED] and with the [REDACTED] record the system time and date, boot sequence and other BIOS (Basic Input/Output System) information. Record this information on both the "[REDACTED]" and the "[REDACTED]". It is important to make note of time/date discrepancies of examined computer equipment. Make note of any time/date discrepancies on both the "[REDACTED]" and the [REDACTED].
5. All "in-house" computer forensic examinations will take place in the [REDACTED]. In an extreme situation where numerous computer systems are to be reviewed, only secured, locked, and approved areas will be used to conduct the examinations. This provision does not apply to cellular/mobile devices.
6. During the course of an examination, it is imperative to ensure that original evidence is not modified in any way. If original evidence is accidentally modified ("stepped on"), the examiner must explain in full detail the event, the cause of the event, the time and date of the event and the results of the event in the final examination report. If a hard drive is damaged before, during or after an examination while in the examiner's chain of custody, the examiner must describe in full detail the events as described above. The examiner must notify his/her supervisor immediately if a hard drive or computer system becomes damaged during the examiner's chain of custody. The damage may not be the

fault of the examiner, but may need to be repaired using Office funds to retrieve evidence or to restore operability to a failed hard drive.

7. It is imperative that the forensic examiner establish and maintain a "sterile" and forensically acceptable working condition. All media that has been forensically imaged / copied will be verified through [REDACTED]. This procedure must be documented in the examination report.
8. Using forensically acceptable software, create "forensic image files" of the media to be examined. Currently, the Morris County Prosecutor's Office utilizes [REDACTED] as the primary computer and cell phone forensics software tools when conducting computer forensic and cell phone forensic examinations.
9. The use of any one or combination of the above software to create images is acceptable. The image files should be named according to the case file number ("X number") assigned to that examination, along with an identifier that specifies the hard drive currently being imaged. Once the images are created, the examiner must verify that the image file(s) match the contents of the original evidence media. This can be accomplished with the use of hash values and software verification processes.
10. Once the [REDACTED] have been verified and accepted, the examiner is required to [REDACTED]. The examiner may optionally test the [REDACTED].
11. The forensic examiner may utilize current forensic procedures to examine [REDACTED]. The examiner must be provided with a suitable amount of time to conduct a proper examination. The examiner must keep in contact with the case detective, assistant prosecutor and/or outside law-enforcement agencies regarding the status of the investigation and provide an approximate time of completion. Often, an examination may take an extraordinary amount of time given the amount of evidence submitted. As such the examiner must maintain contact with the case detectives/assistant prosecutor and make them aware of these delays.
12. Computer equipment cannot be returned to the owner if that computer contains items indicative of child pornography. The examiner must notify the case detective and assistant prosecutor assigned to the case if child pornography is located on a computer or on removable media. It may be the decision of the assistant prosecutor to remove the hard drive before returning the computer or before filing for forfeiture.

13. Cellular phone devices and removable storage devices will be processed in the same manner as computer devices.

a. Computer / Cellular Phone Forensic Examination Reports

- i. Examination report completion typically requires a significantly longer period of time than other forms of investigative reports. Also, one examination of a particular computer system may result in that same computer system being re-examined for different paths of evidence.
 - a) For example, a keyword search on the name "billybob" may result in an email address of billybob@hotmail.com. A search on billybob@hotmail.com returns several documents and spreadsheets with the business name of "Scam, Inc.". The examiner must then search for the keyword "Scam, Inc." etc.
- ii. The examination report must include all descriptions on all evidence found, as well as the procedure used to uncover that evidence. The report is discoverable and it is the responsibility of the forensic examiner to submit a clear, concise, and accurate report.

b. Archiving and Preserving Evidence

- i. There are several methods available to archive and safeguard evidence. As technology develops, higher capacity media and faster methods must be employed to efficiently archive data.
- ii. There will be instances in which entire evidence images must be archived and stored as evidence. These images, if required, can be restored to a wiped and formatted drive or given to defense counsel as discovery upon request.
- iii. Upon the completion of the imaging of evidence, all HTCUC Detectives will archive the [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] At the conclusion of the forensic examination, the investigative exhibits and the [REDACTED]
[REDACTED]
[REDACTED]
- iv. The archiving of forensic evidence files will include, but are not limited to; all [REDACTED]
[REDACTED] etc.

- v. Image files should be properly archived if:
 - The particular computer system (or media) contains items of evidence.
 - The case remains under investigation and is still open.
 - The case involves the death of an individual (homicide, suicide)
- vi. As technology develops, media sources must be adequate enough to properly store information. These media sources which contain image files should be thought of as original evidence and treated accordingly.
- vii. Image files will not be password protected, and must be accessible using the same software used to conduct the examination. A copy of the evidence report will be provided to the case detective. It is incumbent upon the case detective to examine the reports and at times the device in order to identify items of evidential value.

IV. Technical Services

The Technical Services aspect of the High Tech Crimes Unit involves the enhancement and redaction of audio and video files as needed for their use in court and for transcription.

1. All requests for enhancement and redactions must be submitted in writing using the "████████████████████" located on the "C" drive on the network under the "████████████████████". The directions and requirements for enhancements and redactions are located on the form.
2. Additional Technical Services requests which may arise during an investigation and/or trial should be directed to the High Tech Crimes Unit Supervisors for a determination as to whether the technical request is viable, and is within the technical expertise and confines of the equipment and software available to the unit.

V. Training Resources and Certifications

All members of the Morris County Prosecutor's Office High Tech Crimes Unit are encouraged to obtain further training in the area of computer crime, technology and computer forensics. All High Tech Crime Unit Detectives performing computer examinations should be adequately trained in the operation of [REDACTED] [REDACTED] Forensic examiners are encouraged to receive the title of [REDACTED] [REDACTED] or other well-known industry standard or nationally recognized

computer forensic certifications which require specific standards and testing procedures.

The High Tech Crimes Unit will strive to maintain a level of expertise in the fields of high-tech investigations and computer forensics. This will ensure that members of the High Tech Crimes Unit will be able to properly respond to and investigate crimes involving computers and high-tech equipment.