Waukesha Police Memorandum

To: Russell P. Jack, Chief of Police

Attn: Early Shift CID

From: M. Carpenter #405

Date: 04-18-12

Subj: Forensic Server

   I am requesting that the department pursue purchasing a forensic network from Digital Intelligence. There is a definite need for this equipment as outlined below.

   Prior to 2008 digital evidence from an examined computer was stored on DVD or an empty hard drive. This is not a secure and effective way to store sensitive evidence. After Detective Livermore retired I began to purge evidence from old cases. Detective Livermore had several hard drives in his office that contained evidence from older cases. As I was wiping the data from the drives I found that one of the drives had gone bad just by being stored and not used. The evidence on this drive was no longer retrievable. Had this been a current case the evidence would have been completely lost and irretrievable. These cases often involve the most sensitive crimes and the loss of evidence could be devastating to the case.

   After 2008 WKPD began to store evidence on the Waukesha County forensic server. Once we complete a case we store the evidence on their forensic server until it is needed for court or it can be purged. We have the ability to save evidence to the server but we have no other authority to control the server. The administration and security of the server is all handled by the county. We cannot provide any security or integrity of our own evidence. In simpler terms this would be similar to turning our CEFU property room and our drug property room over to another agency and letting them be responsible for our evidence and assuming it will all be accounted for correctly when we need it.

   Also by utilizing the server at Waukesha County lab we are using a large amount of storage space without providing any financial support for it. I am not sure how long this will last. We are currently storing 10 terabytes of data at the county. WKSO contacted me on 04/10/12 and asked that I purge as much evidence as possible due to the amount of space we are using on their server. I also learned today that the county is not utilizing any type of backup software on their server. This means that if their server has some type of failure we will lose all of our evidence with no chance to recover it. We have no ability to back up our evidence at this time. We are currently storing digital evidence from sexual assault, homicide, and child pornography investigations. In many

of these cases digital evidence is the only evidence there is for the case. Several of these cases are still working their way through the judicial system. WKSO advised they are simply storing their evidence on an external hard drive and placing it in a drawer for long term storage. As previously noted this is a dangerous way to store evidence, and not one I recommend we pursue.

We have also greatly increased the amount of computer examinations we are performing, showing the need for our own equipment. In 2009 there were 8 cases, 2010, 44 cases, 2011, 49 cases, and so far in 2012 there have been 17 cases. Based on the number of cases we are performing we need to have our own secure environment to secure our evidence.

The expansion of our departments ICAC (Internet Crimes Against Children) program is also creating a demand for storage space. We will soon be moving to conduct proactive peer to peer file sharing investigation. This is where an investigator can browse the file sharing networks and locate individuals in Waukesha sharing child pornography. The large amount of data we collect during these investigations will have to be stored on a secure network. A forensic server can also be used to store any type of sensitive digital information whether it is a criminal or internal investigation.

While the forensic network is quite expensive, the benefits of it are well worth it. The network would have no bearing on IT's network at WKPD. This server and network are completely self contained. A forensic network cannot connect to the internet or outside world. It can only connect directly to the forensic computers. The only thing WKPD needs to provide is a place to plug the server in. Sensitive material can never be examined on a device that has the ability to access the internet or city network, this is why we cannot simply place our evidence on one of the other servers we use already.

The benefit to purchasing this equipment from Digital Intelligence is the fact that this local company provides lifetime support for training and for the equipment. The sever itself has a one year parts warranty, however in the past Digital Intelligence has extended the warranty on items. I was told that if maintained properly the server would last with no problems 5-10 years. I was told by Digital Intelligence that recently Madison Police Department was using their forensic server well past the suggested lifetime. They suffered a crash and lost all of their sensitive data. Digital Intelligence was able to find older parts and sold them at a discount and subsequently retrieved all of the data that was initially lost. While Digital Intelligence's server may have a higher price tag than others, I am not aware of another company out there that can offer this kind of service under a lifetime warranty. Other manufacturers are also not trained in data recovery and to have this done would have an enormous price tag.

I also talked with Digital Intelligence on how to purchase an item such as this during tight budget times. They offered a 5% discount at the very minimum. I also asked if this payment could be spread out over more than one year and they stated that they would be able to do that. Another possibility would be if we were able to guarantee

funds in the future, would they be willing to provide the system now and receive payment at a later time. The cost for this network is $59,550
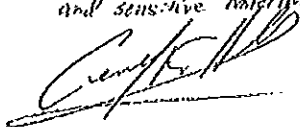
With the purchase of this network Digital Intelligence will provide all of the training necessary to administer the server. If upgrades or changes need to be made to it they will come to our location free of charge to make those changes. They will also retrain another employee if for some reason the Detective currently managing the server was no longer able to do so. This is a great benefit to the Detective's currently working these cases. I do not have the expertise to build my own server and to perform advanced server administration. If we chose to build our own forensic network we would have to figure out another way to do this. It would not be secure to have someone from IT administering our forensic network as the only people that have access to it are the investigators working those cases. There is no way to predict whether or not one of these investigations will lead to another city employee therefore demonstrating the need to have minimal access to this machine.

On 04-18-12 I learned that the server at the WKSO lab had crashed approximately two weeks ago and that county is still trying to recover some of their data. Luckily our data was not affected at this time. I also learned that we will not be able to use our equipment at the county lab for approximately three weeks due to Detective Grall being out on medical leave. Detective Grall is the only person who has access to maintain the server and due to a software upgrade we are unable to use our system. The forensic application FTK was recently upgraded to version 4.0. We are utilizing version 4.0 on the forensic computer at WKPD for our case work, and we must run a matching version at the county lab for the software to work. The newer version of FTK has to connect to a database which is currently stored on the county server. In order for us to use our equipment we need Detective Grall to create an account so that we can access the database.

Respectfully Submitted,

M. Carpenter #405

4-18-12 - I recommend this server be purchased. It is imperative that we maintain and secure our digital evidence. As we move into the future, more digital evidence will be produced at a greater rate. The evidence that we are speaking of is very valuable and sensitive material. Digital Intelligence has proven that it is a trustworthy and reliable company.

6/5/12 Attach To CIP Budget Request for 2013

WAUKESHA POLICE MEMORANDUM

DATE: June 5th, 2012

TO: Russell Jack, Chief of Police

FROM: Ron Oremus, Captain of Police

SUBJECT: Computer Forensic Unit (CFU) Server Request for 2013 Budget/CIP

Attached to this memo is a request from Detective Mike Carpenter from the Computer Forensic Unit as well as a quote for a forensic server. This request is submitted as part of the budget process due to the considerable growth in digital forensic evidence requests and the need to address the issue forensic storage.

Waukesha Police Department currently stores approximately 10 terabytes of our data at the Waukesha County Computer Lab for these types of investigations. It is not uncommon for them to request we purge our cases to make for more room. They also don't have a reliable system in place to back up their data. We currently store highly sensitive information on their system from child pornography cases to evidence from homicide cases. If lost, this could be the difference between defendants walking free or spending years behind bars.

Given our societal dependence on digital devices such as laptops, tablets and smart phones, it stands to reason that our dependence on these devices as valued evidence will also continue to increase. This, coupled with the need to have storage available, a reliable back up and the ability to access this information in an efficient manner has lead to the need for a forensic server.

Forensic servers, however, do not come without a cost. The attached request shows that this server can be installed and maintained by Digital Intelligence for approximately $60,000. This company has worked with us in the past to accommodate our economic situation and this quote is another example of their willingness to work with Waukesha Police Department. Despite the appearance of the cost, a system such as this could be much higher especially if data recovery was factored in. Digital Intelligence is a local company that has expertise in data recovery.

Refer to the attached memo from Detective Carpenter and the quote from Digital Intelligence for further details.

These requests are traditionally split between IT and the CFU part of CID's budget (2140.52240).

Respectfully Submitted,

Ron Oremus
Captain of Police

Digital Intelligence
mastering the science of digital forensics

Digital Intelligence, Inc.
17165 West Glendale Drive
New Berlin, WI 53151

Voice: (262) 782-3332
Fax: (262) 782-3331
Email: sales@digitalintelligence.com

Request for Quote

Date	Quote #
5/8/2012	20120508A

Fed Tax ID # 39-1957034

Customer
Detective Mike Carpenter
Waukesha Police Dept.
Email: Mcarpent@ci.waukesha.wi.us
Tel: 262-524-3923

Item	Description	Quantity	Unit Cost	Total
F6210	Forensic Recovery of Evidence Data Center (FREDC) consisting of:	1	59,550.00	59,550.00
	Forensic File Server (4U) 4U Rackmount Enclosure (10 Bays, 1100W P/S) Dual Intel® Socket 2011 Motherboard for Xeon® processor E5-2600 Product Family. Intel C602-A Chipset. 16 DIMM Slots supporting DDR3 800/1066/1333/1600 Registered ECC memory, Maximum up to 512 GB 6 PCI-Express 3.0 (x16) Slots Two Intel Xeon 5620 (2.4 Ghz, 12 MB) Quad-Core CPU's (8 Processors Total) 32 GB Dual-Channel 128 Bit DDR3-1333 Registered ECC memory 2 ports Intel 6.0 Gb/s Serial ATA (SATA) Controller 8 ports Intel 3.0 Gb/s Serial ATA (SATA) Controller 2 Serial Port Headers 1 RJ-45 port for iKVM (requires ASMB6 card) 2 PS/2 Ports (Keyboard & Mouse)) Four 10/100/1000 MB/s Gigabit Intel® Ethernet Network Adapters 5 USB 2.0 Ports - 2 Back Mounted, 3 Front Mounted Aspeed AST2300 16 MB Graphics Controller 4 port (16 channel) SAS controller card BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive 1.5 TB Internal RAID6 Array (5 X 500 GB Drives) 6.0 TB Internal RAID6 Array (5 x 2.0 TB Drives) 1 x 500 Gb 7200 RPM 3.0 Gb/s SATA Hard Drive in Shock-Mounted tray - Disaster Recovery Drive 1 Shock Mounted Serial ATA (SATA) Removable Hard Drive Bay 2 x RAID Chassis with 5 removable drive bays each (10 total) Yosemite Backup Software Suse Linux Enterprise Server	1		
	32.0 Terabyte RAID Array Module (28 Terabyte RAID-6) (3U) 16-Bay, 3U Rackmount RAID Enclosure (Multilane SAS Attached)	1		

Digital Intelligence

mastering the V science of digital forensics

Digital Intelligence, Inc.
17165 West Glendale Drive
New Berlin, WI 53151

Voice: (262) 782-3332
Fax: (262) 782-3331
Email: sales@digitalintelligence.com

Request for Quote

Date	Quote #
5/8/2012	20120508A

· Fed Tax ID # 39-1957034

Customer

Detective Mike Carpenter
Waukesha Police Dept.
Email: Mcarpent@ci.waukesha.wi.us
Tel: 262-524-3923

16 x 2.0 TB, 7200 RPM Hard Drives in Hotswap removable drive trays				
LTO-5 Ultrium Robotic Tape Library (2U) LTO-5 Ultrium Drive, 16.Slot Library, 1.5 TB (Uncompressed)/ 3.0 TB (Compressed) per tape, Up to 48 TB Total Online Backup Capacity, SAS interface	1			
48 Port Gigabit Ethernet (10/100/1000 MB/S) Rackmount Network Switch (1U)	1			
24 Port Rackmount Network Patch Panel (2U)	2			
3000 VA Rackmount Uninterruptable Power Supply (UPS) (2U)	1			
Forensic Recovery of Evidence Device - RackMount (FRED-RM) (4U)	1			

Intel® Core™ i7-3820 CPU (Quad Processor), 3.6 GHz, 10MB Intel® Smart Cache, 5 GT/s DMI

16 GB PC3-12800 DDR3 1600 MHz Memory [T2007]

1 x 300 GB 10,000 RPM SATA III Hard Drive - OS Drive [T3005]

1 x 2.0 TB 7200 RPM SATA III Hard Drive - Data Drive [T3007]

Windows 7 Ultimate (64 bit) with XP Mode [T0003]
Also includes: DOS (Win98 Standalone), SUSE Professional Linux (64 bit)

Hardware Write Blocking:
Digital Intelligence UltraBay II Hardware Write-Blocker:
- Integrated IDE Drive Write Blocker
- Integrated SATA Drive Write Blocker
- Integrated SCSI Drive Write Blocker
- Integrated USB Write Blocker
- Integrated FireWire IEEE 1394b Write Blocker

Digital Intelligence

mastering the science of digital forensics

Request for Quote

Date	Quote #
5/8/2012	20120508A

Fed Tax ID # 39-1957034

Customer
Detective Mike Carpenter
Waukesha Police Dept.
Email: Mcarpent@ci.waukesha.wi.us
Tel: 262-524-3923

Digital Intelligence Integrated Forensic Media
Card Reader -- Read-Only and Read/Write
switchable

Detailed System Specifications:
4U Rackmount Enclosure (10 Bays)
1100 Watt Modular power supply
17 Motherboard with Intel X79 Express Chipset
6 PCI-Express 3.0(x16)Slots
Nvidia GT 430 1GB GDDR3 PCI-Express Video Card
  with 1 DisplayPort, 1 HDMI, and 1 DVI port -
  supports dual monitors
Dual 10/100/1000 Mbs Intel GbE Network Adapters
8-Channel High Definition Audio CODEC
2 ports Intel 6.0 Gb/s Serial ATA (SATA)
  Controller
4 ports Intel 3.0 Gb/s Serial ATA (SATA)
  Controller - 1 Back Mounted
2 ports Marvell 6.0 Gb/s Serial ATA (SATA)
  Controller
2 PS/2 Ports
6 USB 3.0 ports -- 3 Back Mounted, 3 Front Mounted
13 USB 2.0 ports -- 10 Back Mounted, 3 Front
  Mounted(1 Write Blocked)
1 FireWire IEEE 1394a (400 MB/s) ports - 1 Back
  Mounted
3 FireWire IEEE 1394b (800 MB/s) ports -- 1 Back
  Mounted, 2 Front Mounted(1 Write Blocked)
2 x Shock Mounted SATA Removable Hard Drive Bays
  (IDE Capable)
1 x HotSwap Shock Mounted Universal (IDE/SATA
  compatible) Removable Hard Drive Bays
BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer
  Combo Drive
Extendable/Retractable Imaging Workshelf with
  integrated ventilation

Other Software included: Symantec Ghost, CD
Authoring Software, DRIVESPY, IMAGE, PDWIPE,
PART, and PDBLOCK

Warranty 1 year parts and labor

42U Rackmount Enclosure w/doors and   1
Ventilation Fans - 23.5"(w) x 36"(d) x 84"(h)

Digital Intelligence
mastering the science of digital forensics

Digital Intelligence, Inc.
17165 West Glendale Drive
New Berlin, WI 53151

Voice: (262) 782-3332
Fax: (262) 782-3331
Email: sales@digitalintelligence.com

Request for Quote

Date	Quote #
5/8/2012	20120508A

Fed Tax ID # 39-1957034

Customer
Detective Mike Carpenter
Waukesha Police Dept.
Email: Mcarpent@ci.waukesha.wi.us
Tel: 262-524-3923

B1100	Integrated Rackmount Keyboard/17 inch LCD Display Panel (1U) and 8 port KVM Switch	1		
	KVM over IP Remote Access Module	1		
	Rackmount Rail Kits	4		
	Toolbox containing: Toolbox containing: Adapters, Terminators, Cables, Digital Camera, and Security Screwdriver Set	1		
	Free Training (Limited Time Offer): One Seat per System in the FRED orientation and training course "Digital Forensics with FRED" Please note: Seating is limited and registration is required.	1	0.00	0.00
	Onsite Installation, Configuration, and Equipment Orientation (Continental US)	1	INC	INC
	Standard Electrical Requirements -- FREDC requires a 30 Amp, 120 Volt circuit with a NEMA L5-30R receptacle.			
	Cooling Load: UPS is capable of providing 2700 watts of power at maximum output. This results in a calculated maximum heat output of about 9215 BTU/HR for your Air Conditioning load. Standard build does not saturate UPS.			
	Freight and Delivery charges (CONUS)			DELIVERY
	PAYMENT TERMS: 34% due on delivery 33% after one year 33% after two years			

All prices are in U.S. Dollars

This quote is valid for 30 days from date of issue.

To order please FAX P.O. to (262) 782-3331 or email to sales@digitalintelligence.com

Thank you for your interest

Subtotal	$ 59,550.00
Tax	0.00
Total	$ 59,550.00

Prepared by: Jane Stone / CMG
Rev. 04252012

Police Department Forensic System Questions:

- In the request it was stated that there are three investigators, (Detectives Feyen, Carpenter and Micklitz), are you expanding this system to include additional investigators? If so, are additional workstation(s) included in the request?

- Later in your Forensics File Network response you mention "customers will re-wire connections" -directly at the front panel of the patch panel/48 port switch, which "offers the customers more versatility". Who are these customers? Do you currently have this capability or is this an expansion of the network beyond what we currently have?
- With the criticality stated in the Forensic response, and sensitive nature of losing data so important, why has there not been "bare metal restore" capability added to the system as this has been available in the industry for years now?
- Are there other options available in configuring the system other than those chosen?
- Have you been in contact with any other agencies regarding sharing in the purchase of a system to handle needs?
- Several times it was stated the system is a "closed loop" system. The CIP request also states that the Forensics system cannot be connected to the internet. However in the Q/A response there is mention of a VPN. How this possible if the system is not to be connected to any other outside network?
- The project includes a 48 port switch, this seems to be over kill especially since only three people at the PD are currently utilizing the system now, what will this 48 port switch be used for?
- No data wiring was mentioned anywhere in the quote, was cabling, data jacks, patch cables, etc. to all locations you intend to install included in the quote?
- Since no outside access to external networks are allowed, what devices outside of those being investigated do you intend to connect to?
- Will you be using the same data room as the current City network? If so, will this system plug into the existing electrical environment in the City data room? Was a load calculation done on this to determine if the current electrical/UPS can support it?
- If you are not using the same data center room, is power, cabling, air conditioning/ducting included in the project cost?
- Are you considering a separate wireless network to connect up smart devices? If so how will you deal with the wireless access component of smart devices?

- Can the PD have a representative from the company show up at ITAC to answer additional questions?

Respectfully submitted by the Information Technology Advisory Committee, Alderman Vance Skinner Chair

City of Waukesha   Capital Improvement Project Request

Project Name	Police Dept Computer Forensic Unit Server
Project Number	PD-2013-080

Case#: 412

Submitter Details	Name :Frank DeFranco, Phone :, Email :fdefranc@ci.waukesha.wi.us		
Advocate	Russell Jack		
Initial Cost ($)	$60,000	**Expected Life**	3 Years
Additional Cost ($)	$0	**Project Status**	New
Total Cost ($)	$60,000	**Funding Status**	UnFunded
Project Criticality	Necessity	**New Personnel to be Added**	NO
Cost Code	Computers/Software	**Dept. Project Ranking**	High

Project Cost/Financing Information

Year	Revenue Source 1	Amount 1	Revenue Source 2	Amount 2	Revenue Source 3	Amount 3	Total Amount
2013	City Property Tax	$60,000					$60,000

Impact on Client	LOW - No Impact--organizational unit operations only.
Visibility	LOW - Visible only to internal organizational unit.
Impact on Operations	HIGH - New equipment, system, infrastructure acquisition.
Failure	HIGH -Inability to meet federal or state mandate or City of Waukesha mission.
Regulatory	None
Process Rules	HIGH - Replacement of a mission critical equipment, system, infrastructure.

Project Category	Capital equiment value in excess of 5000
Project Goal	SAFE AND SECURE-1.8 Other ;
Project Outcome	SAFE AND SECURE COMMUNITY-M7 Other ;

Dept Sharing Info	none

Project Purpose	See attached memo

Initial Scope	See attached memo

Sole Source	yes	**Sole Source Vendor**	Digital Intelligence
Sole Source Explanation	See attached memo		

Dept Contact for Prj	Computer Forensic Unit detectives

Time Dept will Spend on Project	1 - 200 hours

City of Waukesha   Capital Improvement Project Request

Project Name   Police Dept Computer Forensic Unit Server

Project Number   PD-2013-080   Case#: 412

Interface Required   No

Project Goals Support   See attached memo